AlterPath™ OnSite Administrator's and User's Guide

Software Version 1.1.0

Cyclades Corporation
3541 Gateway Boulevard
Fremont, CA 94538 USA
1.888.CYCLADES (292.5233)
1.510.771.6100
1.510.771.6200 (fax)
http://www.cyclades.com

Release Date: May 2006
Part Number: PAC0464

Contents

Figures

Tables

Procedures

Chapter 2: Accessing Connected Devices and Managing Power 73

Chapter 7: OSD for All User Types 375

Chapter 8: Miscellaneous Procedures 501

Chapter 9: Troubleshooting 559

Before You Begin

This administrator's and users guide provides background information and procedures for installing, configuring, and administering the Cyclades™ AlterPath™ OnSite and for accessing connected servers and other connected devices.

Audience

This manual is intended for system administrators of the OnSite and for users who may be authorized to connect to devices, to manage power through the OnSite, and to monitor the OnSite's temperature.

This manual describes configuration, administration, and use of the OnSite only. It does not describe how to set up and administer other external services or servers that the OnSite may access for authentication, system logging, IPMI control, SNMP notifications, data buffering, file sharing, or other purposes. This manual assumes that users who are authorized to connect to servers and other devices through the OnSite already know how to use the connected devices.

Document Organization

The document contains the chapters listed and described in the following table.

Table P-1: Document Organization

Chapter Number and Title	Description
1: Introduction	Provides an overview of the features of the AlterPath OnSite along with necessary prerequisite information for understanding the rest of the information in this guide.
2: Accessing Connected Devices and Managing Power	Explains how to access servers and other devices connected to KVM and serial ports and how to manage power through the OnSite.
3. Web Manager Introduction	Explains the common features of the Web Manager and the access prerequisites.
4: Web Manager for Regular Users	Describes how authorized users use the Web Manager to access devices that are connected to ports on the OnSite.
5. Web Manager Wizard	Explains the basic configuration that can be performed by administrative users using the Web Manager Wizard mode.
6: Web Manager for Administrators	Explains how the OnSite administrator uses the Web Manager for managing users port access, and performing other administration tasks.
7: OSD for All User Types	Describes the screens in the Onscreen Display, which can be accessed from a locally-connected keyboard, monitor, and mouse.
8: Miscellaneous Procedures	Provides administration procedures that cannot be performed using the Web Manager.

Table P-1: Document Organization (Continued)

Chapter Number and Title	Description
8: Troubleshooting	Provides troubleshooting procedures.
A: Specifications	Lists specifications and protocols for hardware, security, console management, system management, server management via KVM, upgrades, and additional protocols supported.
B: Advanced Boot and Backup Configuration Information	Provides detailed background information about where boot files reside and how to configure them and about how configuration file changes are managed and how to backup and restore the files.
Index	Provides a way to look up terms. In the online version of this manual, clicking the terms in the index brings you to where they are used in the manual.

Related Documents

The following document for the Cyclades AlterPath OnSite is shipped with the product.

- *AlterPath OnSite QuickStart Guide* (hard-copy)

The following documents for Cyclades AlterPath products mentioned in this guide are on the Documentation CD shipped with the product and are also available at: http://www.cyclades.com/support/downloads.php.

- *AlterPath PM User Guide*
- *AlterPath Manager E2000 Manua*l

Updated versions of this document will be posted on the downloads section of the Cyclades website in the “AlterPath OnSite” section when Cyclades releases new versions of the software.

A hard-copy version of this document can be ordered under part number OST0000-U00 through your Cyclades sales representative.

Typographic and Other Conventions

The following table describes the typographic conventions used in Cyclades manuals.

Table P-2: Typographic Conventions

Typeface	Meaning	Example
Links	Hypertext links or URLs	Go to: http://www.cyclades.com.
Emphasis	Titles, emphasized or new words or terms	See the *AlterPath OnSite Quick Start.*
`Filename or Command`	Names of commands, files, and directories; onscreen computer output.	Edit the `pslave.conf` file.
`User type`	What you type in an example, compared to what the computer displays	`# ifconfig eth0`

The following table describes other terms and conventions.

Table P-3: Other Terms and Conventions

Term or Convention	Meaning	Examples
Hot keys	Hot keys are key sequences that perform certain actions. When hot keys are shown, a plus (+) appears between two keys that must be pressed at the same time, and a space appears between two keys that must be pressed sequentially.	• `Ctrl+k p` entered while the user is connected to a KVM port brings up an IPDU power management screen. `Ctrl` and `k` must be pressed at the same time followed by `p`. • `Ctrl+Shift+i` entered while the user is connected to a serial port brings up the IPMI power management utility. The `Ctrl` key and the `Shift` and `i` keys must be pressed at the same time.
Navigation shortcuts	Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager or OSD screens.	Go to Configuration>KVM> General >IP Users in Expert mode.
\ in a command line example	Used in screen examples when a command does not fit in the space available. Indicates that the whole command should be entered in either of the two following ways: • On one line without the backslash • On multiple lines with a backslash at the end of each line to tell the shell that the command continues on the following line.	`# openssl req -new \ -nodes -key \ private_key.pem \ -out cert.csr`

Additional Resources

The following sections describe how to get technical support, training, and software upgrades.

Cyclades Technical Support

Cyclades offers free technical support. To find out how to contact the support center in your region, go to: http://www.cyclades.com/support/technical_support.php.

Cyclades Technical Training

To learn about the Cyclades Technical Training Center and the courses offered, visit http:www.cyclades.com/training, call 1-888-292-5233, or send an email to training@cyclades.com.

Cyclades Software Upgrades

Cyclades offers periodic software upgrades for the AlterPath products free of charge to current Cyclades customers. You may want to check http://www.cyclades.com/support/downloads.php from time to time to see if upgrades are available for the OnSite or for an AlterPath PM that you may also be using with this product.

See the “Management>Firmware Upgrade” on page 366 for instructions on upgrading the software on the AlterPath OnSite and see “Access>IPDU Power Mgmt.>Software Upgrade” on page 199 for instructions on upgrading the software on any optionally-connected AlterPath PMs.

Chapter 1
Introduction

This chapter gives an overview of the features of the AlterPath OnSite and of how to use the features to securely access and manage connected servers and a large variety of other types of devices.

This chapter also provides important prerequisite information for understanding the information and procedures in the rest of this manual.

The following table lists the topics in this chapter.

Connectors on the AlterPath OnSite

The following table describes the purpose of the connectors on the OnSite. How to connect servers and other devices to the connectors is described in the *AlterPath OnSite Installation Guide*.

Table 1-1: OnSite Connectors and Intended Uses

Connector	Purpose
Serial ports	Connecting servers and other devices that have console ports, and dumb terminals. See “Serial Ports” on page 4.
KVM ports	Connecting servers that have monitors, keyboards, and mice. See “KVM Ports” on page 4.
Modem port	Connecting an active telephone line for dial-in access to the internal modem. (Does not rely on the IP network being up.)
Video, [mouse], [keyboard]—KVM connectors	Connecting a monitor, keyboard, and mouse to create a Local User Station. Once the equipment is connected and the OnSite and the monitor are turned on, an *OSD* (onscreen display) login screen appears and a local user can log in and access its features. See Chapter 7, “OSD for All User Types” for details.
Console port	Connecting the OnSite to a terminal or a computer running a terminal emulator for local management access.
AUX 1 and AUX 2 ports	For any of the following: • Connecting an optional external modem for dial-in access • Connecting an optional CSU/DSU device for dial-in access • Connecting an optional AlterPath PM IPDU or to multiple daisy-chained IPDUs.
Ethernet	Connecting to an Ethernet network for Intranet and Internet access. Both 10BaseT and 100BaseT Ethernet speeds are supported.
PCMCIA card slots	Inserting PC cards providing additional access and storage options, including dial-in access through modem or wireless phone cards.

Serial Ports

Serial ports provide remote access to many types of devices that have console ports.

Servers running Linux, FreeBSD, Solaris, HP/UX, AIX, System V, or other UNIX operating systems, or Microsoft Windows 2003 with emergency management services (EMS) enabled can be managed over their console ports (or serial ports configured as console ports). Through their consoles, you can get low-level control over servers, with access to hardware self-test and BIOS information that is generated before the operating system is loaded and that is therefore not available over the network. Other types of equipment, such as routers, hubs, switches, modems, POS (point-of-sale) systems, PBXs, ATMs, process controllers, and environmental monitoring devices, also have console ports or auxiliary ports that you can connect to the OnSite serial ports for similar purposes.

When a device is connected to an OnSite serial port, you can access diagnostic information (boot messages, error logs, alarms, monitor mode), change low-level system configuration and perform and script other administrative tasks, such as resetting or rebooting the system. You can receive notifications via email, pager, or SNMP trap if a device crashes or other event of interest occurs. You can directly connect to the serial ports via `telnet`, `ssh`, or other connection protocols. You can also connect to the serial ports through the Web Manager.

You can also connect dumb terminals to serial ports. You can dedicate a dumb terminal to a single remote server or you can enable the dumb terminal to access many servers through the OnSite. When configuring a dumb terminal as a local terminal that uses `telnet` or `ssh` to access the OnSite, you can define a command menu that appears when the dumb terminal is turned on.

The OnSite is usually connected to the serial port of a device using a RS-232 cable with a DB-9 connector on the OnSite end.

KVM Ports

The KVM (keyboard, video, mouse) ports provide remote access to the keyboard, monitor, and mouse devices of servers running Microsoft Windows, Sun Solaris and Linux operating systems. Connecting a server to a KVM port allows use of a keyboard, video, and mouse on a remote work station as if it were the keyboard video and mouse of the connected server.

When a KVM port is accessed through the Web Manager the AlterPath Viewer appears and displays the video from the connected server. The connected user can launch applications directly on the server.

KVM connections give real-time access to information that is otherwise inaccessible through in-band network interfaces. For example, BIOS access, POST, and boot messages are inaccessible through inband connections but are accessible through KVM connections. In some cases, the in-band network interfaces are not available after the system boot is completed (for example, after a Windows Safe Mode boot) without the kind of out-of-band access the OnSite provides. An administrator can list and manage processes, add and remove users, and address OS problems even if the GUI is locked or the network is not fully operational.

Overview of OnSite Features

Administration of the OnSite is separate from access to and power management of the connected devices.

Authorized users and administrators can access devices that are connected to the OnSite's ports and manage power, but only administrators can configure access and security on the OnSite. See the following bulleted items for more details.

- Only an OnSite administrator can configure access to the OnSite and to the connected devices.
- OnSite administrators can also access all connected devices.
- Only OnSite administrators can add regular users and authorize them to access ports.
- Regular users can access devices if they are authorized for the ports to which the devices are connected.
- Regular users can manage power outlets on optionally connected AlterPath PM IPDUs if authorized.

The following table lists the security features that administrators can configure to control access to connected devices and to enforce the site's security policies. The table also lists where the features are documented in more detail.

Table 1-2: Security Features and Where Documented

Security Feature	Where Documented
Authentication for accessing the OnSite and connected devices	"OnSite Authentication Options" on page 7
One-time passwords	"One Time Password Authentication on the OnSite" on page 18
Authorizations assigned to users and groups to control access to connected devices	• "Types of Users" on page 19 • "OnSite Port Permissions" on page 32
Security profiles for controlling which network services are turned on or blocked and for setting other security parameters	• "OnSite Security Profiles" on page 22
Logging, *notifications*, and *alarms* that can alert remote administrators about problems, and *data buffering* to capture and monitor user activity.	• "Common Tasks" on page 186 • "To Configure Data Buffering [Wizard]" on page 181 • "SNMP on the OnSite" on page 53 • "To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]" on page 198 • "To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]" on page 198
Encryption of communications between the OnSite and user computers when the users are connected to servers through OnSite KVM ports.	"Encryption" on page 31

OnSite Authentication Options

Anyone accessing the OnSite must log in by entering a username and password. Controlling access by requiring users to enter names and passwords is called *authentication*. The usernames and passwords entered during login attempts are checked against a database that lists all the valid usernames along with their encrypted passwords. Access is denied if either the username or password is not valid.

The password database can reside either locally (on the OnSite) or on an authentication server on the network. Using one or more of the many types of popular authentication methods supported on the OnSite can reduce administrator workload when a user account needs to be added, modified, or deleted.

Note: Even if a remote authentication server is specified, when an administrative user logs in through the Web Manager or through the OSD, then authentication for the administrative user account always falls back to local authentication if the server is not available. For all other types of logins, if an authentication method is specified without a local fallback (such as NIS/DownLocal), and if the authentication server is not available, then authentication fails and the user cannot log in.

Choosing Among Authentication Methods

The administrator can either accept the defaults or select among the many, common, authentication methods available for the following types of access:

- For logins to the OnSite

  The authentication method chosen for the OnSite is used for subsequent access through `telnet`, `ssh`, or the Web Manager. By default, logins to the OnSite use Local authentication.

- For logins to individual serial ports (and connected devices)

  By default, logins to all serial ports use no authentication.

- For logins to all KVM ports (and connected devices)

  By default, logins to the KVM ports use Local authentication

Note: KVM port authentication only applies when KVM ports are configured for direct access and a user accesses the KVM port from the Web Manager login screen.

- For logins over dial-in connections to the OnSite through modems or wireless phone cards.

Local Fallback Options

The authentication methods listed here use both local authentication and authentication servers in the order shown:

- Local/*AuthType*
- *AuthType*/Local
- *AuthType*Down/Local
- *AuthType*Down/Local/Radius

The *AuthType*/Local, *AuthType*Down/Local, and *AuthType*Down/Local/Radius authorization methods are referred to as authentication methods with *local fallback options*.

Local and OTP authentication methods and the authentication methods that have local fallback options require user accounts configured on the OnSite.

If an authentication server for a specified authentication method is down, and a local fallback option is not configured, then authentication fails for regular users. administrative users and for root.

If the authentication server is not available or the user account is not configured properly, then the OnSite administrator needs to work with the authentication server's administrator to fix the problem. If logins to the OnSite are disabled, the root user can use the procedure in "Recovering From Login Failure" on page 2 to fix the lock-out.

Authentication Methods

Note: This section discusses only the types of authentication used for controlling who can access the OnSite and connected devices. Other authentication methods that are used by SNMP, PPTP, IPSec, or PPP are described in the related sections.

The following table lists the supported authentication methods and indicates which methods are available for the OnSite and which are available for devices connected to serial or to KVM ports.

An administrative user can use the Web Manager and any administrator can use the `CLI` utility for configuring an authentication method for the OnSite and for KVM and serial ports and for configuring authentication servers.

The following table lists the supported authentication methods and indicates which methods are available for the OnSite and which are available for devices connected to KVM or serial ports. As mentioned elsewhere, KVM port authentication can only be configured when direct access to KVM ports is configured, and only the “Open” and “Custom” security profiles allow direct access to KVM ports to be configured.

By default, logins to the OnSite and to devices connected to serial ports use Local authentication, and logins to devices connected to KVM ports use no authentication.

All authentication methods except “Local,” “OTP,” and “OTP/Local” require an authentication server, which the administrator configures separately.

When a table cell is blank, the authentication method is not supported.

Table 1-3: Supported Authentication Types (Sheet 1 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
None	No login required.		X [Default]	X
Local	Uses local user/ password for local authentication on the OnSite.	X [Default]	X	X [Default]
Kerberos	Uses user/password configured on the Kerberos authentication server. No logins allowed if Kerberos server is down or Kerberos authentication fails.	X	X	X

Table 1-3: Supported Authentication Types (Sheet 2 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
Kerberos Down/Local	Uses local authentication if Kerberos server is down.	X	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails.	X		X
LDAP	Uses user/password configured on the LDAP (Lightweight directory access protocol) authentication server. No logins allowed if LDAP server is down or LDAP authentication fails.	X	X	X
LDAP Down/Local	Uses local authentication if LDAP server is down	X	X	X
LDAP Down/Local/ Radius	Uses local authentication if LDAP server is down. Uses Radius authentication if local authentication fails.	X		X

Table 1-3: Supported Authentication Types (Sheet 3 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
LDAP/Local	Uses local authentication if LDAP authentication fails	X		X
Local/LDAP	Uses LDAP authentication if local authentication fails	X	X	
NIS	Uses user/password configured on the NIS authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X		X
NIS Down/Local	Uses local authentication if NIS server is down.	X		X
NIS/Local	Uses local authentication if NIS authentication fails.	X		X
Local/NIS	Uses NIS authentication if local authentication fails.	X		X

Table 1-3: Supported Authentication Types (Sheet 4 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
NTLM (Windows NT/ 2000/2003 Domain)	Uses user/password configured on the SMB authentication server (for Microsoft Windows NT/2000/2003 Domain). No logins allowed if SMB server is down or SMB authentication fails.	X	X	N/A
NTLM Down/Local	Uses local authentication if SMB server is down.	X	X	N/A
OTP	Uses the one-time password (OTP) authentication method.			X
OTP/Local	Uses the local password if the OTP password fails			X
RADIUS	Uses user/password configured on the RADIUS authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X	X	X

Table 1-3: Supported Authentication Types (Sheet 5 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
RADIUS Down/Local	Uses local authentication if RADIUS server is down.	X	X	X
RADIUS/Local	Uses local authentication if RADIUS authentication fails.	X		X
Local/RADIUS	Uses RADIUS authentication if local authentication fails.	X		X
TACACS+	Uses user/password configured on the Terminal Access Controller Access Control System (TACACS+) authentication server. No logins allowed if TACACS+ server is down or TACACS+ authentication fails.	X	X	X
TACACS+ Down/Local	Uses local authentication if TACACS+ server is down.	X	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails.	X		X

Table 1-3: Supported Authentication Types (Sheet 6 of 6)

Type	Description	OnSite	KVM Ports	Serial Ports
Local/TACACS+	Uses TACACS+ authentication if local authentication fails.	X		X

Authentication Server Requirements

If configuring any authentication method other than Local, OTP, or OTP/Local, make sure an authentication server is set up for that method. The following list is a summary of the requirements for authentication servers.

- The OnSite must have network access to an authentication server set up for every authentication method specified.
- Each authentication server must be configured and operational.
- The administrator configuring the OnSite needs to work with the administrator of each authentication server to get user accounts set up and to obtain information needed for configuring access to the authentication server on the OnSite.

For example, if LDAP authentication is to be used for logins to the OnSite and if Kerberos authentication is to be used for logins to devices connected to serial ports, then the OnSite needs to have network access to both an LDAP and a Kerberos authentication server, and the administrator needs to perform configuration on the OnSite for each type of authentication server.

Configuration on the OnSite involves supplying the required information to identify the authentication server.

Group Authorization for LDAP, RADIUS, and TACACS+ Authentication

Configuring group authorizations along with LDAP, RADIUS, and TACACS+ authentication adds additional security. When configured for any of the three listed authentication methods, group membership information is retrieved from the authentication server. See “Configuring Groups on LDAP, NTLM, RADIUS, and TACACS+ Authentication Servers” on page 512.

Tasks for Configuring Authentication

Administrative users usually use the Web Manager for configuring authentication. Optionally, OnSite administrators can use one of the following:

- OSD (onscreen display) program
- The `CLI` utility (for configuring authentication for serial ports and for the OnSite but not for KVM ports)

The tasks for configuring authentication are summarized in the following list with links to more information and to procedures using the Web Manager

Table 1-4: Tasks for Configuring Authentication Using the Web Manager

Task	Where Documented
Decide which authentication methods are going to be used for logins to the OnSite and for logins to connected devices.	Table 1-3, “Supported Authentication Types,” on page 9
Make sure an authentication server for each method is accessible to the OnSite and work with the server(s)’ administrators to obtain the information needed to configure the servers on the OnSite and to make sure the required accounts are set up on the servers.	N/A
On the OnSite, configure an authentication server for each authentication method.	“Configuring Authentication Servers” on page 278
Configure the authentication method for OnSite logins or accept the default Local authentication method.	• “Configuration>Security>Authentication” on page 276 • “Configuring Authentication for OnSite Logins” on page 277 • “To Configure an Authentication Type for Direct KVM Port Access” on page 392
Configure the authentication method for serial port access or accept the default Local authentication method.	“To Configure a Serial Port Authentication Method [Expert]” on page 241

Table 1-4: Tasks for Configuring Authentication Using the Web Manager (Continued)

Task	Where Documented
Configure the authentication method for KVM port access or accept the default authentication method of None.	"To Configure an Authentication Method for Direct Access to KVM Ports [Expert]" on page 217 "To Configure an Authentication Type for Direct KVM Port Access" on page 392
Give users the username and password information they need for being authenticated on the devices.	N/A
Configure either a modem, GSM, or CDMA phone PCMCIA card for dial-in logins with OTP authentication, and give users the OTP information they need to be authenticated for dial--ins.	• "Configuration>Network>PCMCIA Management" on page 305 • "To Configure a Modem PCMCIA Card [Expert]" on page 308 • "To Configure a GSM PCMCIA Card [Expert]" on page 312 • "To Configure a CDMA PCMCIA Card [Expert]" on page 318
If you have specified OTP either for one or more serial ports or for dial-ins through modem, GSM, and CDMA PCMCIA cards, configure the OTP authentication method.	"One Time Password Authentication on the OnSite" on page 18

The following table shows the options for configuring authentication using the Web Manager, OSD or `CLI` utility.

Table 1-5: Tasks for Configuring Authentication Methods

Component	Web Manager	OSD	CLI
OnSite Unit	"Configuration>Security >Authentication" on page 276 "To Configure an OnSite Login Authentication Method [Expert]" on page 277	"Configure>Authentication Screens [OSD]" on page 470 "To Configure an Authentication Method and an Authentication Server for OnSite Logins [OSD]" on page 491	`cli> config security authentication`
KVM Ports[1]	"Configuring Authentication for Direct Access to KVM Ports" on page 216 "To Configure an Authentication Method for Direct Access to KVM Ports [Expert]" on page 217	"Configure>General: Authentication Type Screen" on page 391 "To Configure an Authentication Type for Direct KVM Port Access" on page 392	N/A
Serial Ports[2]	"Configuration>Serial/ AUX>Physical Ports> Access" on page 239 "To Configure a Serial Port Authentication Method [Expert]" on page 241	"Configuring Serial Ports [OSD]" on page 446 "To Specify an Authentication Method for Serial Ports [OSD]" on page 450	`cli> config physicalports` [specify "`all`" or a port number from 1-8] `access authtype`

Table 1-5: Tasks for Configuring Authentication Methods (Continued)

Component	Web Manager	OSD	CLI
Modem, GSM, or CDMA PCMCIA Cards (for Dial-in Access)[3]	"Configuration>Network >PCMCIA Management" on page 305 • "Configuring a Modem PCMCIA Card" on page 307 • "Configuring a GSM PCMCIA Card" on page 311 • "Configuring a GSM PCMCIA Card" on page 311	Configure>PCMCIA "To Configure a PCMCIA Card [OSD]" on page 487	`cli> config network pcmcia` [specify a slot number "1" or "2"] [specify `modem | cdma | gsm`] `otpauthreq`

1. Authentication for KVM ports applies only when direct access is configured and only when the user accesses the KVM port directly from the Web Manager login screen. If a user logs into the Web Manager, that user is authenticated using the OnSite's authentication method; the user can then connect to KVM ports without authentication.
2. The authentication method specified for serial ports applies to any attempts to access the serial port.
3. For dial-in access, OTP is the only supported authentication method.

One Time Password Authentication on the OnSite

OPIE (*one-time passwords in everything*) software on the OnSite supports the *one time password* (OTP) authentication method for some types of access.

As noted in Table 1-3 on page 9, the OTP authentication method and the OTP/Local fallback option are supported for serial ports, and the OTP authentication method is supported for dial-ins through modem, GSM, and CDMA PCMCIA cards.

Note: OTP authentication is not supported for logins to the OnSite or to KVM ports.

See Chapter 8, "Miscellaneous Procedures," for how to configure OTP.

Types of Users

The AlterPath OnSite supports three types of users:

- Predefined administrators who can administer the OnSite and its connected devices
- Optionally-added users who can access connected devices through the OnSite
- Optionally-added users who can act as OnSite administrators

Responsibilities of Different User Types

As summarized in the following table, two accounts, root and admin, are configured by default and cannot be deleted. An administrator can also choose to add regular users to the “admin” group, which enables the regular users to perform OnSite administration. The following table lists the responsibilities of each type of user and provides the default password for the root and admin user.

Table 1-6: User Types, Responsibilities, and Default Password

User Name	Responsibilities	Default Password
root	Cannot be deleted. Only console logins allowed. Runs the `wiz` command to do initial network configuration, as described in *AlterPath OnSite Administrator’s and User’s Guide*. Also can run the `CLI` utility and Linux commands on the command line of the Linux shell. Access Privileges: Full Read/Write/Delete/Power Management.	cyclades
admin	Cannot be deleted. Has all access through the Web Manager in Wizard and Expert mode, and through the OSD. Has full access to every function of the Web Manager. Also can run the Cyclades CLI command on the command line of the Linux shell. Access Privileges: Full Read/Write/Delete/Power Management.	cyclades

Table 1-6: User Types, Responsibilities, and Default Password (Continued)

User Name	Responsibilities	Default Password
administrator-assigned	User account optionally configured by an administrator to be able to access devices connected to the ports of the AlterPath OnSite. Regular users can access only those devices that are connected to ports which they have permission to access. Users with permission to access ports or perform certain other tasks through the OnSite are referred to as “authorized users.” Authorized remote users can access either KVM or serial ports through the Web Manager, and authorized local users can access only KVM ports through the OSD. Default Access Privileges for generic users are: No access. Administrators must configure access to ports for any added users. **Note:**If an administrator assigns a regular user to the “admin” group, that user becomes an *administrative user* who can also perform the same administrative functions on the Web Manager as the “admin” user, as described above.	*administrator-assigned*

Parameters for Configuring User Accounts

The OnSite administrator configures user accounts by assigning parameters that are described in the following table.

Table 1-7: User Configuration Settings

Settings	Notes
Username	Login name required for the user account.

Table 1-7: User Configuration Settings

Settings	Notes
Password	Password used for accessing the OnSite.
Group	Regular User Admin (for administrative users)
Shell	Desired shell.
Comments	User information (the UNIX GECOS field)

The administrator can also authorize a user to access devices connected to KVM ports and to manage power outlets on a connected AlterPath PM IPDU.

Configuring Groups

When configuring a group, the administrator can do the following:

- Assign a name to the group
- Assigns users to the group
- Authorize the group to access devices connected to KVM ports

Tasks: Configuring Users

The following table lists the procedures for creating accounts for regular non-administrative users, specifying which KVM ports and serial ports users can access, and specifying which power outlets users can control through the Web Manager

.

Table 1-8: Tasks for Configuring Users

Tool	Where Documented
Web Manager	• "To Add a User [Expert]" on page 294 • "To Assign KVM Ports to a User or Group [Expert]" on page 296 • "To Configure Serial Port Access for Users [Expert]" on page 240 • "To Configure Users to Manage Power Outlets on IPDUs [Expert]" on page 196
OSD	• "To Configure Users [OSD]" on page 459 • "To Add a User [OSD]" on page 460 • "To Give a User Access to KVM Ports [OSD]" on page 463 • "To Configure Who Can Access Serial Ports [OSD]" on page 449 • "To Enable Power Management Through a KVM Port [OSD]" on page 440 • "To Enable Power Management Through a Serial Port [OSD]" on page 448
CLI	• "To Add a User With CLI" on page 545

OnSite Security Profiles

An important part of configuring the OnSite is selecting a security profile that helps enforce the security policies of the organization where the OnSite is being used. The administrative user defines the security profile during initial configuration. The security profile can be changed later.

A security profile must be selected during initial configuration. The security profiles control the following:

- Which services are turned on:
  - FTP
  - HTTP
  - HTTPS

- ICMP
- SSHv1
- SSHv2
- SNMP
- Telnet

- Whether the following types of access are permitted to serial ports:
  - SSH
  - Telnet
  - Raw connection
  - Bidirectional connections
- Whether authentication must be configured for serial ports.
- Whether “Direct access to KVM ports” is available.

  Direct access to KVM ports is available in the Open security profile and is configurable in the Custom security profile. Being available means that configuration of direct access to KVM ports is permitted. If direct access is disabled in the selected security profile, the OnSite administrator cannot configure direct access for KVM ports, the port field does not appear on the login screen.

The following table lists the services and other features that are enabled or disabled or made available or not in the security profiles. All can be configured in the Custom profile.

Table 1-9: Services and Other Functions Defined in Security Profiles (Sheet 1 of 2)

Option
FTP
HTTP & HTTPS Options • Redirect HTTP to HTTPS • HTTP • HTTP port (Assign an alternate port to HTTP; default = 80) • HTTPS • HTTPS port (Assign an alternate port to HTTPS; default = 443)
ICMP

Table 1-9: Services and Other Functions Defined in Security Profiles (Sheet 2 of 2)

Option
IPSec
RPC
SNMP (enables the administrator to configure any version of SNMP)
SSH Options • Allow root login using SSH • SSH v1, SSH v2 (allow or disallow) • SSH Port (assign an alternate port to SSH; default = 22)
Telnet to OnSite
TFTP
Access to Serial Ports • Allow SSH to serial ports • Allow Telnet to serial ports • Allow raw connection to serial ports • Allow bidirectional connection to serial ports • Require authentication to access serial ports
Access to KVM Ports • Allow direct access to KVM ports

The following tables describes the services that are enabled and disabled in the three types of preconfigured security profiles.

Table 1-10 describes the “Moderate” security profile.

Table 1-10: Moderate Security Profile Services/Features

Enabled Services/Features	Disabled Services/Features
HTTP HTTPS Redirect HTTP to HTTPS	FTP

Table 1-10: Moderate Security Profile Services/Features (Continued)

Enabled Services/Features	Disabled Services/Features
ICMP	Default port numbers are not redefined: • HTTP port number = 80 • HTTPS port number = 443
SSH v1 SSH v2	IPSec
• Allow SSH to serial ports • Allow Telnet to serial ports • Allow raw connection to serial ports	RPC
	SNMP (no version allowed)
	SSH root login not allowed
	Default port number is not redefined: SSH port default = 22
	Authentication not required to access serial ports
	Direct access to KVM ports cannot be configured

Table 1-11 describes the “Open” security profile.

Table 1-11: Open Security Profile Services/Features

Option
FTP
HTTP & HTTPS Options • HTTP • HTTP port default = 80 • HTTPS • HTTPS port default = 443
ICMP

Table 1-11: Open Security Profile Services/Features (Continued)

Option
IPSec
RPC
SNMP (any version)
SSH Options • Allow root login using SSH • SSH v1 • SSH v2 • SSH Port default = 22
Telnet to OnSite
TFTP
Access to Serial Ports • Allow SSH to serial ports • Allow Telnet to serial ports • Allow raw connection to serial ports • Allow bidirectional connection to serial ports • Authentication not required to access serial ports
Access to KVM Ports • Direct access to KVM ports can be configured

Table 1-12 describes the “Secured” security profile

Table 1-12: Secured Security Profile Services/Features

Enabled Services/Features	Disabled Services/Features
HTTPS	FTP
SSH v2	• Redirect HTTP to HTTPS • HTTP • HTTP port default = 80 • HTTPS port default = 443

Table 1-12: Secured Security Profile Services/Features (Continued)

Enabled Services/Features	Disabled Services/Features
	ICMP
SSH to serial ports is allowed	Not allowed: • SSH root login • SSH to serial ports • Telnet to serial ports • Raw connection to serial ports • Bidirectional connection to serial ports
Authentication is required to access serial ports	IPSec
Direct access to KVM ports cannot be configured	RPC
	Not allowed: All versions of SNMP SSH v1 SSH port default = 22 Telnet to OnSite

The security profiles can be selected and a custom security profile can be created using any of the following methods:

- Web Manager Wizard, Step 1: Security Profile
  See “To Select or Configure a Security Profile—Wizard” on page 167.
- Web Manager in Expert mode under Configuration > Security Profiles
- CLI command. under config > security > profile

Notifications, Alarms, and Data Buffering

The administrator can configure system logging (*syslogging*), so that messages about the OnSite, any connected IPDUs, computers, or other connected devices can be sent to a syslog server for handling.

The administrator can also configure *data buffering* to store data from communications on serial ports for possible monitoring. If data buffering is enabled the administrator can also configure *alarms* and *notifications* so that remote administrators may be alerted to problems as they occur and notified about server performance, software and configuration changes on devices connected to serial ports.

Data from communications with serial-connected consoles can be stored (buffered) locally, in the OnSite's flash memory, or remotely, either on an NFS server or syslog server.

Syslog Servers

Messages about the OnSite, its connected IPDUs, and other connected devices can be sent to central logging servers, called syslog servers. Console data from devices connected to serial ports can be stored in data buffer files on syslog servers. By default, logging and data buffering are not done.

Syslog servers run operating systems that support system logging services, usually they are UNIX-based servers with the `syslogd` configured.

Prerequisites for Logging to Syslog Servers

Before configuring syslogging, the OnSite administrator must ensure that an already-configured syslog server with a public IP address is accessible from the OnSite. The OnSite administrator must be able to obtain the following information from the syslog server's administrator.

- The IP address of the syslog server
- The facility number for messages coming from the OnSite.

See the following background information about facility numbers, if needed.

Facility Numbers for Syslog Messages

Each syslog server has seven local facility numbers available for its administrator to assign to different devices or groups of devices at different

locations. The available facility numbers are: Local 0 through Local 7. The administrator of your syslog server should assign you a facility number.

For this example, the syslog system administrator sets up a server called “syslogger” to handle log messages from two OnSites. One OnSite is located in São Paulo, Brazil, and the other OnSite is in Fremont, California. The syslog server’s administrator wants to aggregate messages from the São Paulo OnSite into the `local1` facility, and to aggregate messages from Fremont OnSite into the `local2` facility.

On “syslogger” the system administrator has configured the system logging utility to write messages from the `local1` facility to the `/var/log/saopaulo-config` file and the messages from the `local2` facility to the `/var/log/fremont-config` file. If you were in Fremont and identifying the syslog server using the Web Manager, according to this example, you would select the facility number Local 2 from the Facility Number pull-down menu on the Syslog screen (under Configuration>Network>Syslog in Expert mode).

OnSite System Logging Options

The OnSite includes syslog-ng, which can be configured through either the Web Manager or the `CLI` utility to filter messages from the following sources:

- Devices connected to serial (CAS) and AUX ports
- Devices connected to KVM ports
- Buffered data
- Web logs
- System logs

Syslog messages can be sent to the following destinations:

- OnSite console
- The root user
- A syslog server

OnSite Alarm Notifications

The OnSite administrator can configure the OnSite to send alarm notifications about events detected in messages sent by devices connected to serial ports. For sending alarms generated from devices connected to serial ports,

notifications can be configured to be sent to an OnSite administrator by one of the following methods:

- SNMP trap
- Pager
- Email

syslog-ng allows administrators to set up alarm triggers to filter messages based on the messages' facility, level, or contents.

Alarm triggers must be specified in the following format:

```
function("one_or_more_criteria_connected_by_operators");
```

Supported operators are "`and`," "`or`," and "`not`."

The following line shows the syntax for a match function.

```
match("regular_expression_matching_a_text_string");
```

The following line shows the syntax for two match functions connected by the not operator:

```
match("regular_ expression") and not match("regular_
expression");
```

The following example shows the two match functions filtering for logins and excluding messages that have the user name francisco; the functions are connected by the not operator:

```
match("[Ll]ogin") and not match("francisco");
```

For more information, see *syslog-ng v1.6 reference manual* at `http://www.balabit.com/products/syslog-ng/reference-1.6/syslog-ng.html`.

See the following sections for how administrative users can configure notifications and alarms and email:

- "An administrative user can use this screen to enable notifications about system crashes or other events of interest that occur on the device that is connected to the serial port. Data buffering must be enabled. The

administrative user an configure notifications to be sent either by email, pager, or SNMP trap.” on page 268

- “Configuration>Network>Syslog” on page 303

Tasks: Configuring Logging, Alarms, and Data Buffering

The following table lists the procedures related to configuring logging, alarms, and data buffering.

Table 1-13: Tasks for Configuring Logging, Alarms, Data Buffering

To Configure Data Buffering [Wizard]	Page 181
To Add a Syslog Server [Wizard]	Page 183
To Delete a Syslog Server [Wizard]	Page 184
To Configure Data Buffering for Serial Ports [Expert]	Page 243
To Configure Syslogging and Message Filtering [Expert]	Page 304
To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]	Page 198

Encryption

OnSite administrators can specify that communications are encrypted between the users’ computer and the OnSite when the user is connected to a KVM port through the Web Manager. The following table lists the types of encyrption.

Table 1-14: Types of Encryption

Types of Encryption	Description
Level 0	No encryption
Level 1	Encryption of keyboard and mouse data
Level 2	Encryption of video, keyboard, and mouse data
3DES	3DES encryption for levels 1 or 2

See “Configuration>Security” on page 275 for the Web Manager screen and a link to the procedure.

OnSite Port Permissions

In the default configuration, no users except “admin” and “root” can access any ports. The OnSite administrator can configure access for regular users as desired.

The following table summarizes the default port access permissions and default authentication types (Auth Type) and provides links to where the port permissions are described in more detail.

Table 1-15: Default Port Access Permissions

Port Type	Default Access	Default Auth Type	Access Types	Where Documented
KVM	None	None	No access Read only Read/Write Full access (Read/Write/Power management)	“Understanding KVM Port Permissions” on page 32 “To Assign KVM Ports to a User or Group [Expert]” on page 296
Serial	None	Local	None Implicitly: Full (Read/Write/Power management)	“To Configure Serial Port Access for Users [Expert]” on page 240

The OnSite administrator must take the actions described under “Where Documented” to configure any other types of access and authentication than the defaults defined in the previous table.

Understanding KVM Port Permissions

Generic KVM port permissions (which are configured for the “*Generic User”* in the Web Manager and “[*Generic Users*]” in the OSD) apply to all regular users and groups, unless the OnSite administrator configures other permissions for individual users or groups.

KVM port permissions for generic users, for all other types of users and for groups are configured by assigning the following types of permissions:

- *Default permissions* that apply to all KVM ports
- Port access permissions that apply to *individual ports or groups of ports*.

As shipped, the generic users' default permission is "No access." which means that no regular users can access any KVM ports. Editing the Generic User allows you to change the KVM port permissions for all regular users and groups at once.

For generic users, for all other types of users, and for groups, if desired, the OnSite administrator can construct lists of KVM ports with the following types of permissions:

- Ports with no access
- Ports with read only access
- Ports with read/write permission
- Ports with full access (read/write/power)

The OnSite administrator needs to decide which users or groups of users to enable for access to devices connected to KVM ports. To enable users to access KVM ports, the OnSite administrator must do one or both of the following:

- Change the permissions assigned to the Generic User
- Change the permissions assigned to individual users or to groups of users

"KVM Port Permissions Hierarchy" on page 34 provides information the OnSite administrator needs to understand if performing advanced configuration of KVM permissions.

The following table shows the tools that the OnSite administrator can use to set KVM port permissions and where to go for further details.

Table 1-16: Tools for Setting KVM Port Permissions

Tools	Where Documented
Web Manager	"Setting KVM Port Permissions" on page 291 and "To Assign KVM Ports to a User or Group [Expert]" on page 296.
OSD	"Configure>KVM Ports Screens [OSD]" on page 436

KVM Port Permissions Hierarchy

An administrator can give the same access to every user by modifying the Default Permission and also by specifying permissions for individual ports or groups of ports for the Generic User. Before trying to configure more fine-grained control of users' access to ports, the administrator needs to understand how the system handles requests from a user who is trying to access a KVM port. The series of decisions is shown in a flow chart in Figure 1-1 and examples are provided in the following sections.

Decision 1: Check User's KVM Port Permissions

1. Does the user have specific KVM port permissions for the requested port?
    - If yes, the specified permissions apply: no access, read-only, read-write, or read/write/power management.
    - If the user has no specific KVM port permissions, go to Decision 2.

Example for Decision 1

- If user john is trying to access KVM port 4 and his account has port 4 in a list of ports with full permission, then john is given read/write and power management access.
- If user jane is trying to access KVM port 4 and her account has port 4 in a list of ports with no permission, then jane is denied access.
- If users jim, joan, jerry, jill, joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and do not have port 4 listed for any types of access, then their access requests are passed to Decision 2.

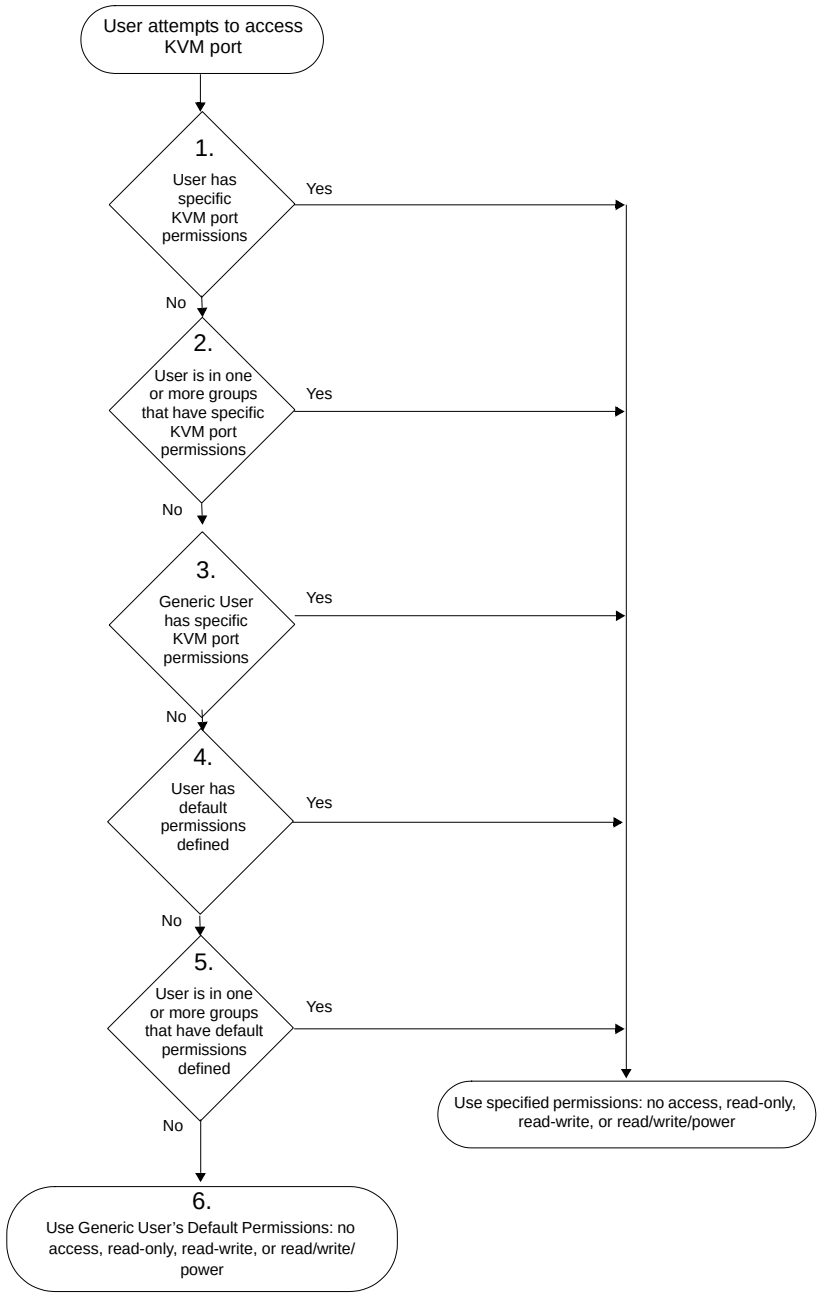


Figure 1-1: KVM Port Permissions Hierarchy

Decision 2: Check Group's KVM Port Permissions

2. Is the user a member of a group with specific KVM port permissions for the requested port?
   - If yes, the specified permissions apply: no access, read-only, read-write, or read/write/power management.
   - If a user is in more than one group with specific KVM port permission, the permissions are ANDed, and the most restrictive permission is used.
   - If the user is not in a group or is in a group with no specific KVM port permissions, go to Decision 3.

Example for Decision 2

- If user jim who is trying to access port 4 is a member of three groups, and the first group's permission is "rwp," the second group's permission is "rw" and the third group's permission is "ro," the result of ANDing all three permissions is "ro," and jim is given read-only access.
- If user joan is trying to access port 4, and she is in a group called linux_ca3 that has port 4 in a list of ports with no permission, then joan is denied access.
- If jerry and jill are trying to access port 4, and they are in a group called linux_ca4 that has no specific port permissions defined, then their access requests are passed to Decision 3.
- If joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4, and they are not in any group, then their access requests are passed to Decision 3.

Decision 3: Check Generic User's KVM Port Permissions

3. Does the Generic User have specific KVM port permissions for the requested port?
   - If yes, the specified permissions apply: no access, read-only, read-write, or read/write/power management.
   - If no, go to Decision 4.

Example for Decision 3

- If user jerry is trying to access port 4, and the Generic User has port 4 in a list of ports with full access permissions, then jerry is given read writer and power management access.
- If user jill is trying to access port 4, and the Generic User has port 4 in a list of ports with no access permissions, then jill is denied access.
- If users joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4, and the Generic User does not have port 4 listed for any type of access, then their access request are passed to Decision 4.

Decision 4: Check User's Default Permissions

4. Does the user have a Default Permission for the requested port?
   - If yes, the specified permissions apply: no access, read-only, read-write, or read/write/power management.
   - If the user has no Default Permission, the user is under the Generic User's default permission, and the request for access goes to Decision 5.

Example for Decision 4

- If user joe is trying to access port 4, and he has a Default Permission that allows read only access to ports, then joe is given read only access.
- If user jennifer is trying to access port 4, and she has a Default Permission that allows no access to ports, then jennifer is denied access.
- If users jordan, jolanda, and jezebel are trying to access port 4, and their Default Permissions are under the Generic User's Default Permission, then their access requests are passed to Decision 5.

Decision 5: Check Group's Default Permissions

5. Does the user belong to a group that has a Default Permission for the requested port?
   - If yes, the specified permissions apply: no access, read-only, read-write, or read/write/power management.

- If no, go to decision 6.

Example for Decision 5

- If user jordan trying to access port 4 is in a group called windows_ca1 that has a Default Permission of full, then jordan is given read/write and power management access.
- If user jolanda trying to access port 4 is in a group called windows_ca2 that has a Default Permission of no access, then jolanda is denied access.
- If user jennifer is not a member of any group with a Default Permission specified, then her access request is passed to Decision 6.

Decision 6: Check Generic User's Default Permissions

Note: If an access request gets this far, the Default Permission of the Generic User is the only permission that could apply.

---

6. What are the Default Permission for the Generic User?

   The specified permissions apply: no access, read-only, read-write, or read/write/power management.

Support for Multiple Types of Access

The OnSite provides multiple types of remote and local access described in this section.

Remote OnSite Access Options

Remote OnSite administrators and authorized users can connect remotely in the following ways:

- Using the Web Manager in a browser from LANs, WANs, GSM or CDMA cell phones, either through the Ethernet port or a PPP or login

dial-in connection to the internal modem, optional phone or wireless cards in the PCMCIA slots, or one or two optional external modems

- Using applications such as `telnet` or `ssh` to connect to the console of devices that are connected to the OnSite's serial ports
- Using PPP or a terminal emulation program to dial into a modem (with optional callback), get console access to the OnSite, and through the `CLI` utility either perform administration, access connected devices, or run power management commands.

Remote OnSite administrators can also do the following to connect to and administer the OnSite itself.

- A remote administrative user logged into the Web Manager can launch a console session from the first screen that comes up after login and be automatically logged into the OnSite console as admin. The default shell defined for admin is `bash`. The administrative user can run the `wiz` command and the OnSite command line application (called the *CLI).*
- The administrative user connected to the OnSite console cannot switch users to root but can use the `sudo` command to run commands that need to run as root. For example, to run the `reboot` command that can only be run by root, the admin can enter: `sudo reboot`.
- A remote administrator using `telnet` or `ssh` can connect to the OnSite and log in as root.

Local OnSite Access Options

The OnSite provides several types of *direct connection options.*

- Logins to the OSD from a local monitor, keyboard, and mouse (also called a Local User Station) directly connected to the KVM management port

  By connecting a *local user* station (consisting of a monitor, keyboard, and mouse) directly to the Local User ports on the OnSite, OnSite administrators and authorized users can use the *Onscreen Display* (OSD). When the monitor and the OnSite are turned on, the OSD login screen appears on the monitor.

- Logins using a terminal or terminal emulator from a direct connection to the console management port.

By connecting a terminal or computer running a *terminal emulation program* to the console port, an OnSite administrator can log into the OnSite as root and can enter commands from the on-board Linux command line or the OnSite `CLI` utility in the Linux shell.

D*umb terminals* can also be connected to any serial port and configured as follows:

- Dedicated to access one specific server
- A menu can be configured that allows the connected user to access any number of servers

Access Options Table

The following table lists the access methods with links to where they are described.

Table 1-17: OnSite Access Methods

Access Method	Where Documented
LAN, WAN	• "Browser Access With the Web Manager" on page 42 • Chapter 3, "Web Manager Introduction" • Chapter 4, "Web Manager for Regular Users" • Chapter 6, "Web Manager for Administrators"
phone line	• "Dial-in Access Types and Options" on page 41
`telnet`, `ssh`	• Chapter 2, "Accessing Connected Devices and Managing Power"
OSD	• "Chapter 7, "OSD for All User Types
dumb terminal	• "Serial Port Connections" on page 100 • Table 6-13, "Protocols for Dumb Terminals Connected to Serial Ports," on page 233.

Dial-in Access Types and Options

Authorized users can dial into the OnSite through any of the three following types of devices:

- Internal modem
- Optional external modem connected to an AUX port
- Optional modem PCMCIA card
- Optional GSM or CDMA phone PCMCIA card

All types of modems or phone cards can be accessed through PPP when the following prerequisites are done:

- The modem has been configured for PPP on the OnSite end.
- The PPP application at the remote caller's end has been configured for dial-in and optional callback access.

A PCMCIA modem or other phone card can also be accessed for login access from a terminal emulation program. Once you plug in the modem card and connect it to a dedicated phone line, no configuration is needed to enable dial-in access. However, for callback to work, the OnSite administrator must configure the modem or phone card for callback.

The following list provides links to the section and procedures for connecting to modems.

The following table lists the modem installation and configuration procedures for the three types of modems, with links to where they are documented.

Table 1-18: Tasks for Modem Installation and Configuration

Modem Type	**Where Documented**
Internal modem	• "To Configure the Internal Modem [Expert]" on page 267
External modem	• "To Configure an AUX Port for PPP [Expert]" on page 266
PCMCIA modem or wireless phone card	• "To Configure a Modem PCMCIA Card [Expert]" on page 308 • "To Configure a GSM PCMCIA Card [Expert]" on page 312 • "To Configure a CDMA PCMCIA Card [Expert]" on page 318

Browser Access With the Web Manager

Both OnSite administrative users and authorized users can access the Cyclades Web Manager from a supported browser.

The OnSite administrator can use the Web Manager to configure users and ports and security. An authorized user can access connected devices through the Web Manager to troubleshoot, maintain, cycle power, and reboot connected devices. An authorized user can also use the Web Manager to manage power outlets on optionally connected AlterPath PM IPDUs, monitor the OnSite's temperature, and change their own passwords, but they do not have access to the OnSite screens for configuring users or ports. For details about using the Web Manager, see:

- Chapter 3, "Web Manager Introduction"
- Chapter 5, "Web Manager Wizard Mode"
- Chapter 6, "Web Manager for Administrators"
- Chapter 4, "Web Manager for Regular Users"

Port Access Prerequisites

Connecting to a port and accessing a server or other device requires the following.

- The user needs the username and password for a user account defined on the server or other device.
- To administer a device, the user needs root or administrator access.
- For other uses of a connected device, the user needs a regular user account on the device or on an authentication server, if authentication is enabled for the device.

Conditions for KVM Port Access

Access to KVM ports through the Web Manager is sometimes referred to as *KVM over IP*. KVM over IP is supported by IP modules installed in the OnSite. If the OnSite's model number ends with "1," the OnSite has one IP module. If the model number ends with "2" the OnSite has two IP modules. See the *AlterPath OnSite Installation Guide* for a list of all the OnSite models and their model numbers.

The maximum number of IP connections (by remote users) is four. Two types of IP connections are supported:

- KVM over IP
- Inband

KVM Over IP

Depending on the model, one or two users can have KVM over IP access through the Web Manager or the OSD, as described in the following list:

- OnSite models with one IP module allow connection to KVM ports by either one "admin" OR one regular user.
- OnSite models with two IP modules allow two connections to KVM ports by either one "admin" AND one regular user OR by two regular users.

Inband

AdaptiveKVM on the OnSite makes use of Microsoft Remote Desktop Protocol (RDP) technology. RDP is included on all new Windows servers by default.

After configuration, AdaptiveKVM provides network-efficient *inband* connections as long as the server is operational. When the Windows server is fully operational, the RDP protocol is used to provide access to the server. If the server is not fully operational and is not accepting RDP connections, AdaptiveKVM uses the KVM over IP connection to provide uninterrupted access to the managed device.

Inband connections are only available when a Windows server with RDP enabled is connected to a KVM port. Both the server and the OnSite must be connected to the same network.

For more details see the Tech Times newsletter on Adaptive KVM Technology at http://www.cyclades.com/newsletter/articles/tech20050801.

The OnSite supports up to four concurrent inband connections, with the number reduced by the number of KVM over IP connections simultaneously in existence. The maximum number of IP connections is four, and KVM over IP connections count against the total of connections allowed, so, for example, if one KVM over IP connection exists, then only three inband connections can be made at that same time.

Local User Station

A local user can access a KVM port through the OSD using a directly-connected keyboard, video, and mouse (called a “Local User” station).

Additional Conditions

For accessing KVM ports and using the AlterPath Viewer through the Web Manager, the following additional conditions apply:

- The computer must have a 500 MHz Pentium III processor or greater.
- The computer must be running the Windows NT 4.0, XP, 2000, or ME operating system.
- The browser must be Internet Explorer 6.0 and above.
- The ActiveX plug-in must be enabled in the browser for the AlterPath Viewer to work
- Mouse settings on the server must be configured properly for the user’s mouse movements to be synchronized with the server.

Conditions for Serial Port Access

If port sharing is not enabled, then one user at a time can access a device connected to a serial port.

If port sharing is enabled, multiple users can simultaneously access a device connected to a serial port. If two users have write access, only the first of the simultaneously connected users can write to the device. The second user who connects to the port gets read only access.

For accessing serial ports using the Java applet viewing window, the Java 2 Runtime Environment (J2RE) or later must be installed on the computer and the Java plug-in must be registered with the browser being used. See the *AlterPath OnSite Installation Guide* for details.

Port-access Related Procedures in the Installation Guide

Procedures for enabling the ActiveX plug-in in the browser, configuring the correct mouse settings on the servers, and enabling the Java plug-in are provided in the *AlterPath OnSite Installation Guide*.

Direct Access to KVM Ports and KVM Port Authentication

The OnSite administrator can enable direct access to all KVM ports, so that authorized users can directly log into KVM ports through the Web Manager login screen. If direct access to KVM ports is enabled, a “port name” field appears on the Web Manager login screen, as shown in the following figure.

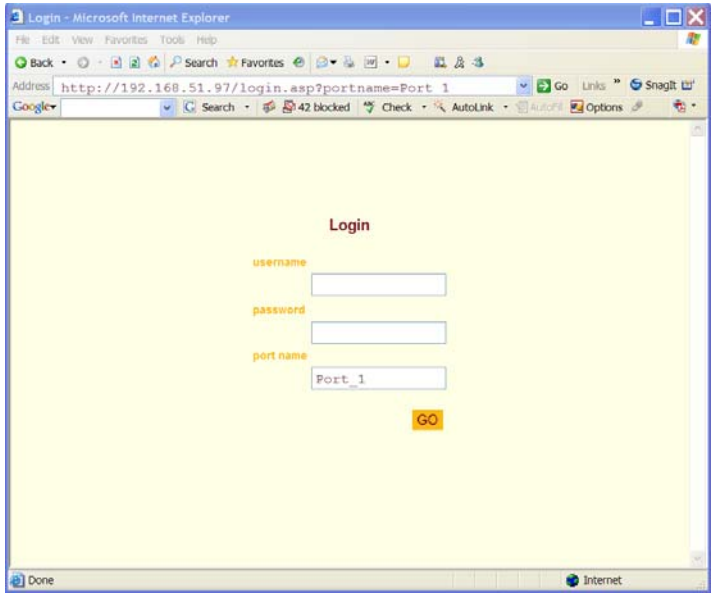


Figure 1-2: Web Manager Login Fields With KVM Port Direct Access Enabled

The OnSite administrator can also configure an authentication method that applies to all KVM ports when the following conditions are true:

- The administrator has configured the KVM ports for direct access
- The user accesses the KVM port from the Web Manager login screen.

If a user logs into the Web Manager before connecting to a KVM port, that user is authenticated using the OnSite's authentication method; the user can then connect to KVM ports without authentication.

Direct access can only be enabled if the OnSite's security profile allows it. Only the "Open" and "Custom" security profiles allow direct access to KVM ports to be configured.

The options for configuring direct access to KVM ports in the Web Manager and in the OSD are listed in the following table, which provides links to more information.

Table 1-19: Tasks for Configuring Direct Access to and Authentication for KVM Ports

OSD	• "Configure>General: Direct Access Screen" on page 394 • "To Enable Direct Access to KVM Ports [OSD]" on page 394 • "To Configure an Authentication Type for Direct KVM Port Access" on page 392
Web Manager	• "Enabling Direct Access to KVM Ports" on page 214 • "To Enable Direct Access to KVM Ports [Expert]" on page 214 • "To Configure an Authentication Method for Direct Access to KVM Ports [Expert]" on page 217

Port Numbers and Aliases

Each connected device is identified in different ways in the management software by the port number to which it is connected.

The following table shows the default conventions for addressing the device files and port numbers for the AUX ports, KVM ports, serial ports, and PCMCIA slots on the OnSite.

Table 1-20: Port Numbers, Names, Device Filenames, TCP Port Numbers

Port or Slot	Number	Port Name on Web Manager	Device File Name	TCP Port Number
AUX	1-2	N/A	`ttyA`[1 | 2]	N/A
Modem (internal)	3	N/A	`ttyA3`	N/A
Console	0	N/A	`ttyS0`	N/A

Table 1-20: Port Numbers, Names, Device Filenames, TCP Port Numbers (Continued)

Port or Slot	Number	Port Name on Web Manager	Device File Name	TCP Port Number
KVM	1-8	Port_*n*	`ttyK`*n*	When a user connects to a KVM port through the Web Manager (KVM over IP), the AlterPath Viewer uses port 5900 by default. If a second IP module exists, port 5901 is used for a second KVM over IP session.
Serial	1-8	Port *n*	`ttyS`*n*	7001-7008, 3000 (for the pool of serial ports)
PCMCIA	1-2		`ttyM`*n*	N/A

The TCP port numbers for serial ports are used when a user connects to a serial port using `telnet` or another connection protocol or when a user connects to the serial port through the Web Manager. When a user connects to a serial port, the Java applet uses the TCP port that is assigned to the port number, for example port 7001 is assigned to serial port 1.

The TCP port numbers for KVM ports are used by the AlterPath Viewer when a user connects to a KVM port over the network. By default, when a user connects to a KVM port over the network, the AlterPath Viewer uses port 5900. If a second IP module exists, port 5901 is used for the second AlterPath Viewer launched over IP. You can assign a different port number or numbers through the OSD or the web management interface. Do not assign reserved TCP port numbers 1 through 1024.

Special circumstances may require OnSite administrators to configure TCP port numbers different from the defaults. For example, a firewall may block TCP port 5900 or 5901.

The OnSite administrator can assign a descriptive alias to each port to identify the connected computer. For example, if a SunBlade server is connected to KVM Port_3, the administrator could define Port_3's alias to be "SunBlade," so "Port_3" is replaced in the ports list by "SunBlade."

Note: The list of ports in the OSD displays only 19 characters. If anyone will be using the OSD for KVM port access, keep this in mind. If longer aliases are required at your site, put the information that uniquely identifies the server at the beginning of the alias.

The following table provides links to procedures for changing default TCP port numbers and port aliases.

Table 1-21: Tasks for Configuring TCP Port Numbers and Port Aliases

Task	Where Described
Change the TCP port number assigned to the Java applet	"To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console [Expert]" on page 254
Change the TCP port number(s) assigned to the AlterPath Viewer(s)	"To Configure Local User Sessions [Expert]" on page 221 "To Configure IP Users (KVM Over IP) Sessions [Expert]" on page 222 "Configure>KVM Ports Screens [OSD]" on page 436
Assign an alias describing the server connected to the KVM port	"To Configure an Alias for a KVM Port [Expert]" on page 226
Assign an alias describing the device connected to the serial port	"To Configure an Alias for a Serial Port [Expert]" on page 238

Power Management

OnSite administrators and users who are authorized for power management can power off, power on, and reboot devices through the OnSite.

Options for Managing Power

Authorized users can perform power management through the OnSite in the following ways:

- From screens in the Web Manager
- From screens in the OSD
- Using power management commands on the command line while logged into the OnSite console
- From a power management screen or dialog while logged into a device through a KVM or serial port

The OnSite provides the following two types of power management options:

- IPMI power management
- IPDU power management

IPMI Power Management

Intelligent Platform Management Interface (IPMI) power management allows authorized users to control power for servers with IPMI controllers (also referred to as IPMI devices), which respond to IPMI commands over the network.

The OnSite supports the following two types of IPMI power management:

- Authorized users can manage power for IPMI devices through the Web Manager. For this type of IPMI power management, the IPMI device does not need to be physically connected to the OnSite, but the OnSite.needs network access to the device.
- Authorized users can also manage power for an IPMI device while logged into the device through a serial port to which the IPMI device is physically connected

IPDU Power Management

IPDU power management allows authorized users to control power for devices that are plugged into an AlterPath PM intelligent power distribution unit (IPDU), when the IPDU is connected to one of the OnSite's two AUX ports and properly configured.

Multiple AlterPath PM intelligent power distribution units (IPDUs) can be daisy-chained to allow power management of up to a total of 128 outlets per AUX port. Since both AUX ports can be used for IPDU power management, you can plug in and manage up to 256 devices.

When a device is physically connected to either a serial port or KVM port and plugged into an IPDU, authorized users can manage power for that device while connected to a serial or KVM port to which the device is physically connected.

When a device with multiple power supplies is connected to a serial port, the device can be plugged into multiple outlets on daisy-chained IPDUs, and authorized users can managed all outlets as a group.

Power Management While Connected to Devices

Authorized users can do the following types of power management while connected to a device through one of the OnSite's ports:

- Users can perform IPDU power management of a connected server while logged into the server through a KVM port.
- Users can perform IPDU or IPMI power management of a connected device while logged into the device through a serial port.

Power Management from the OnSite Command Line

OnSite administrators can use the following commands to manage power:

- The `pm`, `pmCommand` commands for performing IPDU power managment
- `ipmitool` commands to manage power on IPMI devices.

The `pm` and `pmCommand` commands are introduced in "Managing IPDU Outlets With PM Commands" on page 119.

Power Management Configuration Tasks

See the following table for power management configuration tasks and where they are described.

Table 1-22: Tasks for Configuring Power Management

Task	Where Documented
Configure an AUX port for IPDU power management	"To Configure an AUX Port for IPDU Power Management [Expert]" on page 266
Configure multi-outlet power control	Table 6-4, "Tasks for Configuring Multi-Outlet Control," on page 203
Configure users for IPDU power management	"To Configure Users to Manage Power Outlets on IPDUs [Expert]" on page 196
Configure servers for IPMI power management	"To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management [Expert]" on page 206
Configure ports for power management by connected authorized users	"To Configure a Serial Port for IPDU or IPMI Power Management [Expert]" on page 250 "To Configure a KVM Port for Power Management [Expert]" on page 225 "Configure>KVM Ports Screens [OSD]" on page 436 "Configure>Serial Ports Screens [OSD]" on page 440

OnSite administrators can use the `CLI` command to configure power management. The following table shows some example commands.

Table 1-23: Example CLI commands for Power Management Configuration

Task	CLI Command
Configure IPMI device	`config ipmi` *`IPMIdevicename`*

Table 1-23: Example CLI commands for Power Management Configuration

Task	CLI Command
Configure a serial port for IPDU power management	`config physicalports` *`portname`* `powermanagement enable`
Configure a serial port for IPMI power management	`config physicalports` *`portname`* `powermanagement enableIPMI server` *`IPMIdevicename`*

SNMP on the OnSite

The OnSite administrator can activate Simple Network Management Protocol (SNMP) agent software that resides on the OnSite so that the SNMP agent sends notifications about significant events or traps to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager. The OnSite SNMP agent supports SNMP v1, v2 and v3.

The following table shows the tasks related to administering SNMP on the OnSite and provides links to where they are documented.

Table 1-24: Tasks for Configuring SNMP

Task	Where Documented
Configure SNMP	“Configuration>Network>SNMP” on page 323
	“To Configure SNMP [Expert]” on page 326
Activate the SNMP service	“Configure>Network>SNMP Screens [OSD]” on page 400
Configure one or more serial ports to send SNMP traps	“To Configure a Trigger for SNMP Trap Notification for Serial Ports Expert]” on page 272

VPN on the OnSite

The OnSite administrator can set up VPN (Virtual Private Network) connections to establish encrypted communications between the OnSite and an individual host or all the hosts on a remote subnetwork. The encryption creates a security tunnel for communicating through an intermediate network that is untrustworthy.

A security gateway with the IPsec service enabled must exist on the remote network. The IPsec gateway encrypts packets on their way to the OnSite and decrypts packets received from the OnSite. A single host running IPsec can serve as its own security gateway. The OnSite takes care of encryption and decryption on its end.

Connections between a machine like the OnSite to a host or to a whole network are usually referred to as *host-to-network* and *host-to-host tunnel*. OnSite host-to-network and host-to-host tunnels are not quite the same as a VPN in the usual sense, because one or both sides have a degenerated subnet consisting of only one machine.

The OnSite is referred to as the Local or “Left” host, and the remote gateway is referred to as the Remote or “Right” host.

The following figure shows a single host running IPsec acting as its own security gateway on the right end and the OnSite acting as its own gateway on the left end.

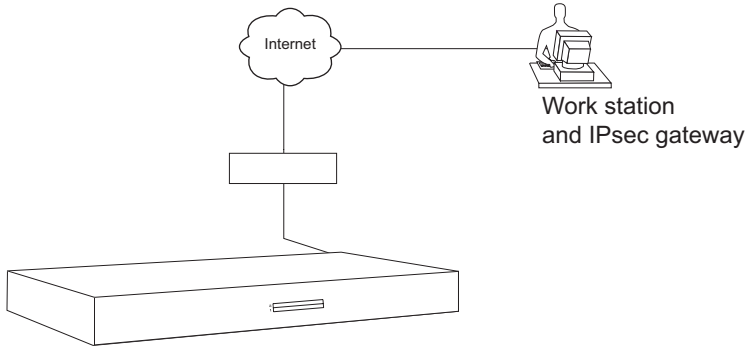


Figure 1-3: OnSite VPN Example

In summary, you can use the VPN features on the OnSite to create the two following types of connections:

- Create a secure tunnel between the OnSite and a gateway at a remote location so every machine on the subnet at the remote location has a secure connection with the OnSite.
- Create a secure tunnel between the OnSite and a single remote host

The gateway in the former example and the individual host in the second example both need a fixed IP address.

To set up a security gateway, you can install IPsec on any machine that does networking over IP, including routers, firewall machines, various application servers, and end-user desktop or laptop machines.

The ESP and AH authentication protocols are supported. RSA Public Keys and Shared Secret are also supported.

The following table describes the parameters that must be configured for a VPN connection. The left column gives the names used in the Web Manager and the OSD separated by a slash, unless the names are the same. Work with the user who needs to make the VPN connection to make sure the information matches exactly on both ends.

Table 1-25: Field and Menu Options for Configuring a VPN Connection

Parameter Names: Web Manager/OSD	Definition
Connection Name	Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN.”
Authentication Protocol/Protocol	The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header).
Authentication Method	Authentication method used, either “RSA Public Keys” or “Shared Secret.”
Boot Action	The boot action configured for the host, “Ignore,” “Add,” and “Start.” “Ignore” means that VPN connection is ignored. “Add” means to wait for connections at startup. “Start” means to make the connection.

Table 1-25: Field and Menu Options for Configuring a VPN Connection (Continued)

Parameter Names: Web Manager/OSD	Definition
ID	The hostname of the host. The local host is the OnSite, referred to as the "left" host. The remote host is referred to as the "right" host.
IP Address/Local IP	The IP address of the host.
NextHop	The router through which the OnSite (on the left side) or the remote host (on the right side) sends packets to the host on the other side.
Subnet Mask/Subnet	The netmask of the subnetwork where the host resides.
RSA Key (If RSA Public Keys is chosen)	The public key for the OnSite and for the remote gateway. You can use copy and paste to enter the key in the "RSA Key" field.
Pre-Shared Secret (If "Shared Secret" is chosen)	Pre-shared password between left and right users.

The following table provides links to related information and procedures.

Table 1-26: VPN Configuration Topics

Topic	Where Documented
Configure VPN	"Configuration>Network>VPN Connections" on page 320
	"To Configure VPN [Expert]" on page 322
	"Configure>Network>VPN Screens [OSD]" on page 403

Monitoring Temperatures

Anyone authorized to log into the OnSite can view graphical displays of temperature readings taken from three embedded temperature sensors. Users can also modify graph display settings, create graph profiles, and apply a stored profile to the current graph.

The temperature sensors are located at the following locations within the OnSite:

- FPGA (field programmable gate array)[
- Power supply
- CPU

The following figure shows an example graph.

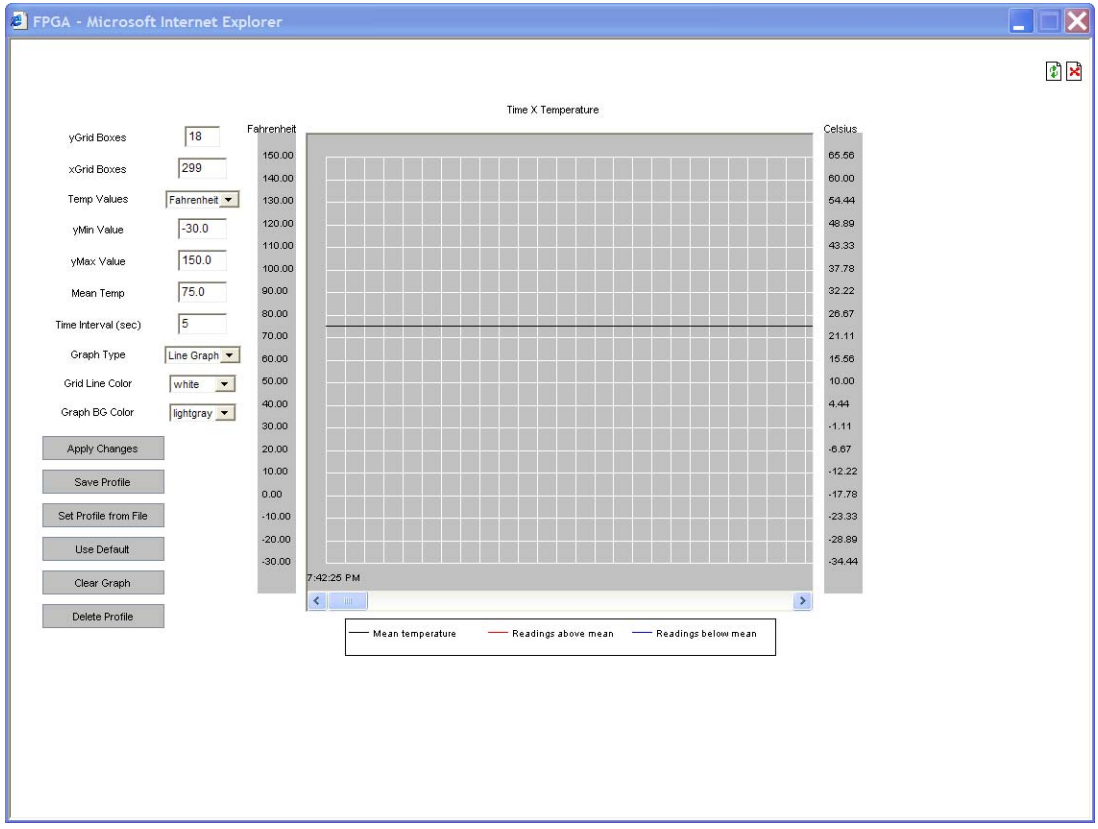


Figure 1-4: Temperature Sensor Graph

The graph displays new readings at a specified interval. The interval between temperature readings is shown in each graph's heading.

The following table shows graph features that can be saved in reusable profiles.

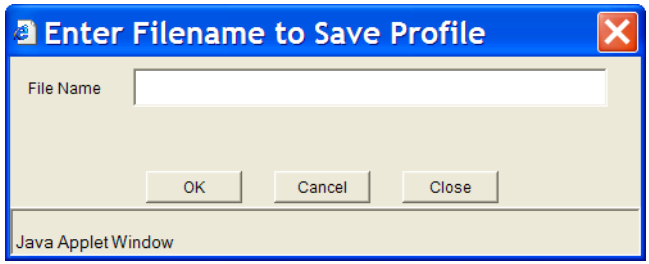
Table 1-27: Temperature Graph Parameters

Field/Menu	Use	Default	Allowed Values
yGrid Boxes	Specify a different number of rows	18	1-55
xGrid Boxes	Specify a different number of columns Each graph cell represent the interval between readings.	299	1-999
Temp Values	Specify one of two temperature values.	Farenheit	• Farenheit • Celsius
yMin Value	Specify a different minimum value to display on the y-axis.	-30°F/ -5°C	-196.6°F/ -127°C
yMax Value	Specify the maximum value to display on the y-axis.	150°F/ 50°C	260.6°F/ 127°C
Mean Temp	Specify a different temperature to use as a basis for comparing the actual temperature. In line graphs, the Mean Temp is indicated by a red, horizontal line. In bar graphs, the colors of the bars indicate the following: • Blue – Less than mean temperature. • Red – Greater than mean temperature. • Black – Equal to the mean temperature.	75°F/ 25°C	-196.6°F/ -127°C to 260.6°F/ 127°C
Time Interval (sec)	Set a time interval in seconds.	5	

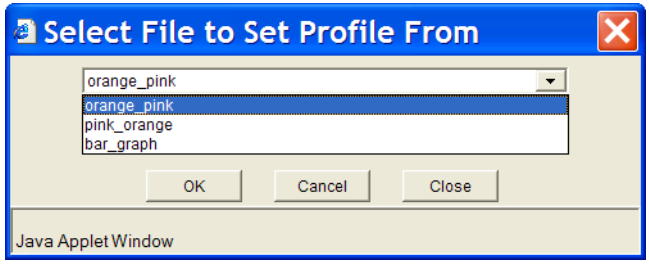
Table 1-27: Temperature Graph Parameters (Continued)

Field/Menu	Use	Default	Allowed Values
Graph Type	Chose another graph type.	Line Graph	• Line Graph • Bar Graph
Grid Line Color	Choose another color for the lines.	white	• yellow • green • cyan • gray • darkgray • lightgray • magenta • orange • pink • white
Graph BG Color	• Select the background color.	light gray	

You can create one or more profiles that store a set of display parameters you specify, so that you can apply the same profile later. Clicking “Save Profile.” brings up the “Enter Filename to Save Profile” dialog box shown in the following figure.



In the “File Name” field, you can enter a name for a profile. When you click OK, the profile is saved in a list of profiles that appears when you click the “Set Profile from File” button.



For how the OnSite administrative and regular users can monitor temperatures, go to “To Monitor the OnSite’s Temperature” on page 158.

Administering Users of Connected Devices

This section reviews the tasks that OnSite administrators need to do to enable access to connected devices.

Planning Access to Connected Devices

Planning should include the following steps:

- Create a list of servers and other devices to connect to each port.
- If devices are going to be plugged into outlets on connected IPDUs, make a note of the outlets where the devices will be plugged (you need to supply the outlet numbers when configuring power management).
- Create a list of user accounts with the access each user needs to which ports and to which IPDU outlets.

- Obtain usernames and passwords for connected devices to give to the users of connected devices.
- Create meaningful aliases to assign to port numbers to identify the devices to be connected

Tasks for Configuring Connected Devices

During hardware installation of the OnSite, the installer connects the servers and devices and any IPDUs and modems to the ports.

During software configuration, the OnSite administrator does the common tasks in the following table, if desired.

Table 1-28: Tasks for Configuring Access to Connected Devices

Task	Where documented
Assigns aliases to ports and to IPDU outlets to identify the connected servers and devices	• "To Configure an Alias for a KVM Port [Expert]" on page 226 • "To Configure an Alias for a Serial Port [Expert]" on page 238
Creates accounts for regular non-administrative users, specifies which KVM ports and serial ports users can access, and specifies which power outlets users can control through the Web Manager.	• "To Add a User [Expert]" on page 294 • "To Assign KVM Ports to a User or Group [Expert]" on page 296 • "To Configure Serial Port Access for Users [Expert]" on page 240 • "To Configure Users to Manage Power Outlets on IPDUs [Expert]" on page 196
Configures authentication methods for access to the OnSite, to all KVM ports and to individual serial ports or groups of serial ports.	• "To Configure an OnSite Login Authentication Method [Expert]" on page 277 • "To Configure an Authentication Method for Direct Access to KVM Ports [Expert]" on page 217 • "To Configure a Serial Port Authentication Method [Expert]" on page 241

Table 1-28: Tasks for Configuring Access to Connected Devices (Continued)

Task	Where documented
Chooses the connection protocol for serial ports [Default=Console (telnet)]	• "To Configure a Serial Port Connection Protocol for a Console Connection [Expert]" on page 236 • "To Configure a Serial Port Connection Protocol for a Dumb Terminal [Expert]" on page 237 • "To Configure a Serial Port Connection Protocol for a Dumb Terminal [Expert]" on page 237

At any time the OnSite administrator can do the common tasks in the above table or do the less-common tasks listed below.

Table 1-29: Tasks for Redefining Hot Keys and TCP Port Numbers

Task	Where documented
Redefine keyboard shortcuts (hot keys) if desired	• "Configuring Keyboard Shortcuts (Hot Keys)" on page 63
Redefine TCP port numbers used for accessing serial and KVM ports, if desired	• "To Configure IP Users (KVM Over IP) Sessions [Expert]" on page 222 • "To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console [Expert]" on page 254

Configuring Keyboard Shortcuts (Hot Keys)

Predefined keyboard shortcuts (also called hot keys) allow users to do the following:

- Perform common actions while connected through a KVM or serial port
- Emulate Sun keyboard keys while connected through a KVM port to a Sun server.

Configuring KVM Port Connection Hot Keys

The hot key sequences that can be used while connected to a KVM port have two parts, which are called the *common escape sequence* and the *command key*. The default common escape sequence is `Ctrl+k`, and the command key is different for each command. For example, the `q` command key is entered after `Ctrl+k` to quit, as in: `Ctrl+k q`.

The common escape sequence is defined separately from the command keys. OnSite administrators can redefine two different sets of command keys for users who are accessing KVM ports in the two following different ways:

- Through the OSD (Local Users)
- Through the Web Manager (KVM over IP Users)

Note: The “Show Connections” dialog on OnSite hardware version 1.1.0 replaces the hot keys for KVM over IP sessions on OnSite hardware version 1.0.0. See “What You See When Connected to a KVM Port” on page 82 for details.

Configuring Serial Viewer Hot Keys

Connecting to a serial port brings up a Java applet viewer. The hot key used to bring up an IPDU power management window in the Java applet viewer is `Ctrl+p`. The hot key used to bring up an IPMI power management window is `Ctrl+Shift+i`.

Configuring Sun Keyboard Equivalent Hot Keys

The OnSite provides a default set of hot keys for use while connected to Sun servers through KVM port to emulate keys that are present on Sun keyboards but are not present on Windows keyboards. The hot keys are made up of an escape key followed by a function key.

See “Sun Keyboard Emulation Hot Keys” on page 87 for more details. The default escape key is the Windows key, which is labeled with the Windows logo. OnSite administrators can redefine the Sun emulation escape key to be one of the following: `Ctrl`, `Shift`, or `Alt`.

Tasks for Configuring Hot Keys

See the following table for tasks for configuring hot keys with references to where they are documented.

Table 1-30: Tasks for Redefining Hot Keys

Part	Web Manager: Where Documented	OSD: Where Documented
KVM common escape sequence	“To Redefine KVM Port Connection Hot Keys [Expert]” on page 215	“Configure>General Screens [OSD]” on page 389
KVM command keys for the local user session	“To Redefine KVM Port Connection Hot Keys [Expert]” on page 215	“Configure>User Station Screens [OSD]” on page 427
KVM command keys for IP user sessions (only on OnSite hardware version 1.0.0)		N/A
Serial power management hot key	“To Configure a Serial Port for IPDU or IPMI Power Management [Expert]” on page 250	

Table 1-30: Tasks for Redefining Hot Keys (Continued)

Part	Web Manager: Where Documented	OSD: Where Documented
Sun keyboard emulation escape key	"To Redefine the Escape Key for Sun Keyboard Emulation Hot Keys [Expert]" on page 216.	"Configure>KVM Ports Screens [OSD]" on page 436

Packet Filtering on the OnSite

The OnSite administrator can configure the OnSite to filter packets like a firewall. IP filtering is controlled by *chains* and *rules*.

Chains

A chain is a kind of named profile that includes one or more rules that define the following:

- A set of characteristics to look for in a packet
- What to do with any packet that has all the defined characteristics

The OnSite comes with a number of built-in chains. The OnSite administrator can define additional chains and can edit the built-in chains. The built-in chains are named according to the type of packet they handle, as shown in the following list:

- INPUT - For incoming packets
- FORWARD - For packets being routed through the OnSite
- OUTPUT - For outgoing packets

As defined in the rules for the default chains, all input and output packets and packets being forwarded are accepted.

Rules

Each chain can have one or more rules that define the following:

- The packet characteristics being filtered

  The packet is checked for characteristics defined in the rule, for example, a specific IP header, input and output interfaces, TCP flags and protocol.

- What to do when the packet characteristics match the rule

  When a packet is filtered, its characteristics are compared against the rules one-by-one. All defined characteristics must match.

Administrators can do the following to specify packet filtering:

- Add a new chain and specify rules for that chain
- Add new rules for existing chains
- Edit or delete built-in chains and rules

Add Rule and Edit Rule Options

When you add or edit a rule you can define any of the options described in the following table.

Table 1-31: Filter Options for Packet Filtering Rules

Filter Options	Description
Source IP and Mask **Destination IP and Mask**	If you specify a source IP, incoming packets are filtered for the specified IP address. If you specify a destination IP, outgoing packets are filtered for the specified IP address. If you fill in a source or destination mask, incoming or outgoing packets are filtered for IP addresses from the subnetwork in the specified netmask.

Table 1-31: Filter Options for Packet Filtering Rules

Filter Options	Description
Protocol	You can select a protocol for filtering from one of the following options: • ALL • "Numeric Protocol Options" on page 67 • "TCP Protocol Options" on page 68 • "UDP Protocol Options" on page 68 • "ICMP Protocol Options" on page 68
Input Interface	The input interface (eth*N*) used by the incoming packet.
Output Interface	The output interface (eth*N*) used by the outgoing packet.
Fragments	The types of packets to be filtered: • All packets • 2nd, 3rd... fragmented packets • Non-fragmented and 1st fragmented packets

You can flag any of the above elements with *inverted* so that the target action is performed on packets that do not match any of the criteria specified in that line. For example, if you select DROP as the target action, specify "Inverted" for a source IP address, and do not specify any other criteria in the rule, any packets arriving from any other source IP address than the one specified are dropped.

Numeric Protocol Options

If you select Numeric as the protocol when specifying a rule, you need to specify the desired number.

TCP Protocol Options

If you select TCP as the protocol when specifying a rule, you can define the following options.

Table 1-32: TCP Protocol Packet Filtering Options

Field/Menu Option	Definition
Source Port - OR - **Destination Port**	You can specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. You can also specify a second number, so that TCP packets are filtered for any port number within the range starting with the first number and ending with the second.
TCP Flags	Specifying any of the flags: “SYN” (synchronize), “ACK” (acknowledge), “FIN” (finish), “RST” (reset), “URG” (urgent) or “PSH” (push), and one of the “Any,” “Set,” or “Unset” conditions, filters TCP packets for the specified flag and the selected condition.

UDP Protocol Options

When you select UDP as a protocol when specifying a rule, you can select the UDP options defined in the following table.

Table 1-33: UDP Protocol Packet Filtering Options

Field	Definition
Source Port - OR - **Destination Port**	Specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. You can specify a source or destination port number for filtering in the “Source Port” field. You can also specify a second number so that UDP packets are filtered for any port number within the range.

ICMP Protocol Options

When you select ICMP as a protocol when specifying a rule, you can select the following ICMP options.

- all
- echo-reply

- destination-unreachable
- network-unreachable
- host-unreachable
- port-unreachable
- fragmentation needed
- source-route-failed
- network-unknown
- host-unknown
- network-prohibited
- host-prohibited
- TOS-network-unreachable
- TOS-host-unreachable
- communication-prohibited
- host-precedence violation
- precedence-cutoff
- source-quench
- redirect
- network-redirect
- host-redirect
- TOS-network-redirect
- echo-request
- router-advertisement
- router-solicitation
- time-exceeded
- ttl-zero-during-transit
- ttl-zero-during-reassembly

Target Actions

The “Target” is the action to be performed on an IP packet that matches all the criteria specified in a rule.The target actions are:

- ACCEPT
- DROP

- RETURN
- LOG
- REJECT

If the “LOG” and “REJECT” targets are selected, additional options are available.

The following table describes the options for the “LOG” Target.

Options	Definition
Log Level	emerg alert crit err warning notice info debug
Log Prefix	The prefix to use in the log entry.
TCP Sequence	Includes the TCP sequence in the log.
TCP Options	Includes TCP options in the log.
IP Options	Includes IP options in the log.

The following list shows the options for the REJECT Target:

- icmp-net-unreachable
- icmp-host-unreachable
- icmp-port-unreachable
- icmp-proto-unreachable
- icmp-net-prohibited
- icmp-host-prohibited

- echo-reply
- tcp-reset

Firewall Configuration Procedures

The following table has links to the procedures for defining packet filtering using the Web Manager.

For information about defining packet filtering in the OSD, see “Configure>Network>IP Filtering Screens [OSD]” on page 408.

Chapter 2
Accessing Connected Devices and Managing Power

This chapter gives an overview of the options for accessing servers and other devices that are connected to the ports on the OnSite and for performing power management through the OnSite.

The following table lists the topics in this chapter.

The following table lists the procedures in this chapter.

Options for Accessing Connected Devices

Authorized users are users who have been authorized to access one or more ports on the OnSite. See “OnSite Port Permissions” on page 32 and “OnSite Port Permissions” on page 32 for more information.

Note: Only one administrative user can be logged into the CLI, Web Manager, or OSD at a time. If another administrative user is logged by any means, the second administrative user attempting access is prompted either to exit or to proceed and log the other administrative user out.

Authorized users and OnSite administrators have the following options accessing devices:

- Web Manager—for accessing devices connected to both KVM and serial ports

  See Chapter 3, “Web Manager Introduction” for background information about the Web Manager; Chapter 6, “Web Manager for Administrators” for how OnSite administrative users can access ports through the Web Manager; and Chapter 4: “Web Manager for Regular Users” on page 139 for how authorized users access ports through the Web Manager.

- `telnet` or `ssh`—for accessing devices connected to serial ports

  See “Serial Port Connections” on page 101 and “To Use Telnet to Connect to a Device Through a Serial Port” on page 104, for more information.

- Onscreen display (OSD)—for accessing devices connected to KVM ports

  Local users and administrators who have access to a directly-connected Local User station can access the Connection Menu through the OSD. See

Chapter 7, “OSD for All User Types” for how to access connected devices through the OSD.

- Dumb terminal—for accessing the OnSite or devices connected to serial ports through the OnSite

  See “To Connect Through a Dumb Terminal to a Server or to the OnSite” on page 102.

- Modem or PCMCIA modem or wireless phone card—for dial-in/callback access to the OnSite through PPP or a terminal emulator

  See “Support for Multiple Types of Access” on page 38, for the types of modems supported. Also see “To Start a PPP Connection From a Remote Computer” on page 115 and “To Dial Into the OnSite Using a Terminal Emulator” on page 117.

Power Management

As mentioned in “Power Management” on page 50, OnSite administrators and users who are authorized for power management can power off, power on, and reboot devices through the OnSite.

The following table lists the options for OnSite administrators and regular users for performing power management.

Table 2-1: Power Management Options in the Web Manager

Type	Where Documented
IPDU power management	For administrative users: • "Access>IPDU Power Mgmt." on page 193 • "To View Status, Lock, Unlock, Rename, or Cycle Power Outlets" on page 150 • "To View and Reset IPDU Information [Expert]" on page 153 For authorized users: • "IPDU Power Mgmt. [User]" on page 148 • "To Power On, Off, or Cycle a Server While Connected to a KVM Port" on page 100 • "To Manage IPDUs from the Command Line as Root" on page 120 • "Power Management Through the OSD" on page 382 • "Power Management Menu [OSD]" on page 384 • "To Power On, Power Off, Lock, Unlock, or Cycle Power Outlets [OSD]" on page 385
IPMI power management	For administrative users: • "Access>IPMI Power Mgmt." on page 204 For authorized users: • "To Manage Power While Connected to a Serial Port" on page 107

Using the AlterPath Viewer

Connecting to a KVM port through the Web Manager brings up an AlterPath Viewer.

The first time the AlterPath Viewer appears, a dialog box appears and prompts the user to accept a Security Certificate.

If no one else is logged in, a login screen or prompt from the server appears like the example in Figure 2-1. If the user exits the AlterPath Viewer without logging out of the server, the login persists until the next time a connection is made to the server, unless the server or another user has closed the session.

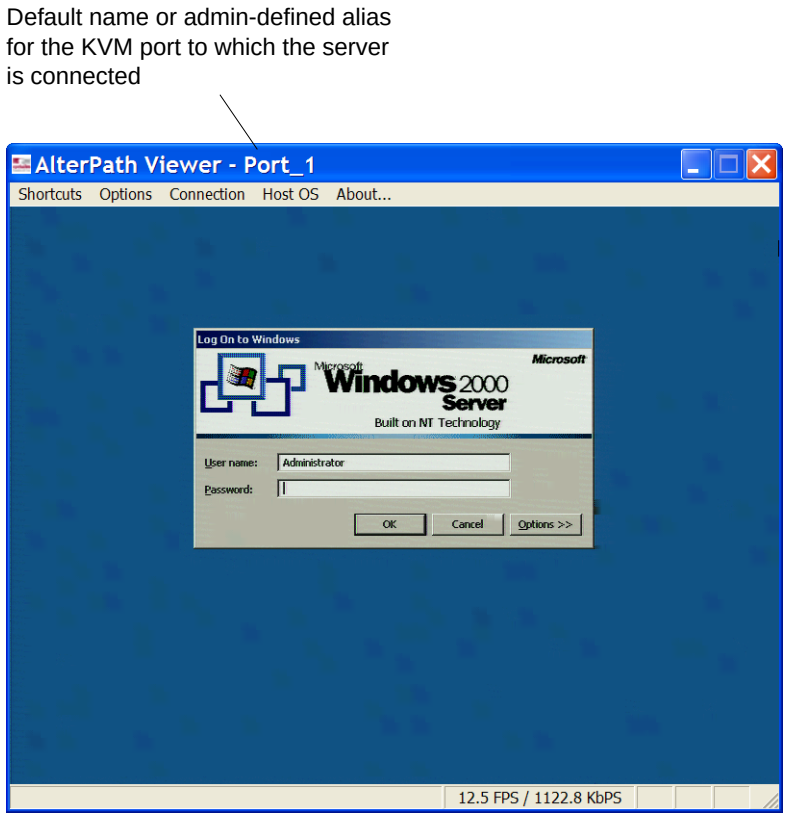


Figure 2-1: AlterPath Viewer

The default port name or administratively-defined alias displays in the viewer title bar, as shown in Figure 2-1.

Ending an AlterPath Viewer Session

The four ways you can end an AlterPath Viewer session are listed below:

- Select “Exit Viewer Client” from the AlterPath Viewer Shortcuts menu.
- Use a hot key sequence (`Ctrl+k q`) to bring up the Connection menu, then select the “Exit” option.
- Let the session time out.
- Click the `Esc` key.

Configuring the AlterPath Viewer

You can configure the AlterPath Viewer settings from the top menu on the viewer. For a definition of the menu settings, refer to the sections listed in the following table.

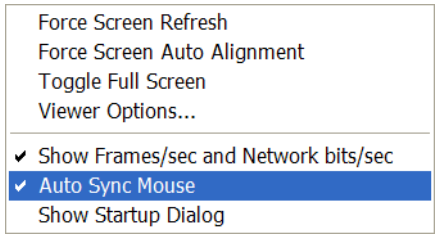
Recommended AlterPath Viewer Settings

The recommended AlterPath Viewer settings for best performance and image quality are listed in the following table. The connection option you select must reflect your actual Internet connection method.

Menu	Select the following option(s):
Options	Auto Sync Mouse
Connection	LAN (preferred), No Encryption, High Color
Host OS	Auto/Other

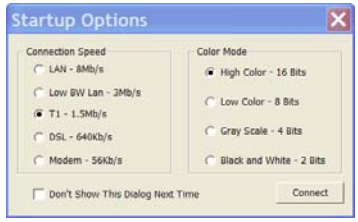
AlterPath Viewer Options Menu

The AlterPath Viewer’s Options menu is shown in the following figure.



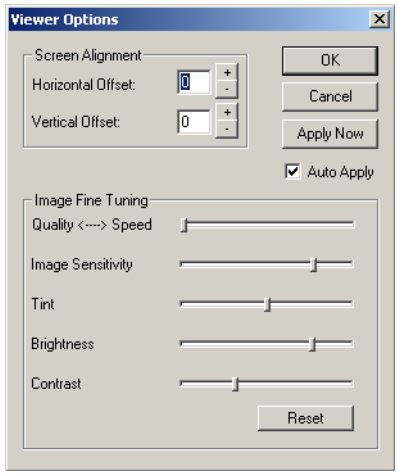
The following table describes the items in the Options menu, which you can change as needed for your own requirements.

Table 2-2: AlterPath Viewer Options Menu

Menu Selection	Description
Force Screen Refresh	Refreshes the viewer.
Force Screen Auto Alignment	Switches to Auto Alignment mode, which may change the position of the viewer. (You can manually configure Screen Alignment by going to Options>Viewer Options>Screen Alignment.)
Toggle Full Screen	Switches the viewer's display from window to full-screen mode or from full-screen to window mode.
Viewer Options	See "Setting the AlterPath Viewer Options" on page 81.
Show Frames/sec and Network bits/sec	Shows the data transfer rates from the server to your workstation at the bottom right of the AlterPath Viewer window.
Auto Sync Mouse	Make sure this is selected for OnSite compatibility.
Show Startup Dialog	Causes the following menu to appear when the viewer is launched. 

Setting the AlterPath Viewer Options

The Viewer Options window allows you to align or position the viewer window and to fine tune the image. The configuration for these settings may vary from one system to another.



The following table defines the fields and menu items.

Table 2-3: AlterPath Viewer>Options>Viewer Options Menu

Field or Menu Item	Function
Horizontal Offset	The horizontal coordinate for positioning the AlterPath Viewer on the screen (default = 0).
Vertical Offset	The vertical coordinate for positioning the AlterPath viewer on the screen (default = 0).
Quality <---->Speed	Move slider to the left to increase image quality; move slider to the right to increase the performance of the viewer.
Image Sensitivity	Move slider to the right to increase the image sensitivity.
Tint	Move the slider to achieve the desired color. For white, keep the slider in the middle.
Brightness	Move the slider to the right to increase screen brightness.

Table 2-3: AlterPath Viewer>Options>Viewer Options Menu

Field or Menu Item	Function
Contrast	Move the slider to the right to increase screen contrast.

AlterPath Viewer Connection Menu

The following table describes the AlterPath Viewer Connection menu options.

Table 2-4: AlterPath Viewer Connection Menu Options

Menu Selection	Function
56K	For when the network connection method is a 56K modem
DSL	For when the network connection method is a DSL line
T1	For when your network connection method is a dedicated T1 line
Low BW LAN	Limits the bandwidth usage to 2Mbps for a local area network where available bandwidth is low
LAN	For when you are connecting through a standard speed local area network.
Auto	For auto detection and setting of the connection mode
Encrypt Everything	Encrypts mouse, keyboard, and video data
Encrypt Keyboard and Mouse	Encrypts only keyboard and mouse data
Encrypt Type	Choices are either RC4 or Triple DES encryption
No Encryption	Video, mouse, and keyboard data are not encrypted [Recommended]
High Color	For high color resolution screens

Table 2-4: AlterPath Viewer Connection Menu Options (Continued)

Menu Selection	Function
Low Color	Limits color depth to use less bandwidth
Gray Scale	Limits bandwidth usage
Low Gray Scale	Limits bandwidth to the minimum

What You See When Connected to a KVM Port

When anyone connects to a KVM port, if no one else is logged in, a login screen or prompt from the server appears like the example in the following figure.

Figure 2-2: What You See When Connected to a KVM Port

If a user exits the AlterPath Viewer or OSD without logging out of the server, the login session persists until the next time a connection is made to the server, unless the server or another user has closed the session.

Figure 2-2 shows an example login dialog for a Windows 2000 server. If a connection is made to a Linux server without a graphical display, a “Login” prompt appears.

Shortcuts While Connected to KVM Ports

Three types of shortcuts allow authorized users connected to a KVM port to perform common actions, and in some cases the shortcuts launch screens for performing certain tasks.

As summarized in the following table, the “Show Connections” dialog is available through the Web Manager with the OnSite hardware version 1.1.0. If the “Show Connections” dialog is available, the other two options listed below do not work in the AlterPath Viewer:

- The Print Screen key
- Predefined keyboard shortcuts (hot keys)

Both the Print Screen key and KVM port hot keys always work for local users connected to the Local User ports to the OSD.

Table 2-5: Show Connections Dialog Availability in OnSite Hardware Versions

	AlterPath Viewer	OSD	Where Documented
“Show Connections” Dialog	1.0.0 h/w: N 1.1.0 h/w: Y	1.0.0 h/w: N 1.1.0 h/w: N	“Show Connections Link and Dialog” on page 146
Print Screen key	1.0.0 h/w: Y 1.1.0 h/w: N	1.0.0 h/w: Y 1.1.0 h/w: Y	“Print Screen Key” on page 85
Predefined keyboard shortcuts (hot keys)	1.0.0 h/w: Y 1.1.0 h/w: N	1.0.0 h/w: Y 1.1.0 h/w: Y	“KVM Port Shortcut Hot Keys” on page 86

The “Show Connections” Dialog is available with the newest version of OnSite hardware. (See “Show Connections Link and Dialog” on page 146.) If the link is available, the other two options listed below do not work in the AlterPath Viewer, but both options always work for local users connected to the Local User ports to the OSD.

The two following options are available in the AlterPath Viewer only if the “Show Connections” dialog is not available.

- The Print Screen key
  See “Print Screen Key” on page 85.
- Predefined keyboard shortcuts (also called hot keys)
  See “KVM Port Shortcut Hot Keys” on page 86.

Print Screen Key

The Print Screen key gives you access to most of the actions that can be accessed by the hot keys. (The key has different labels on different keyboards, such as “Prt Scr” and “Prt Sc.”)

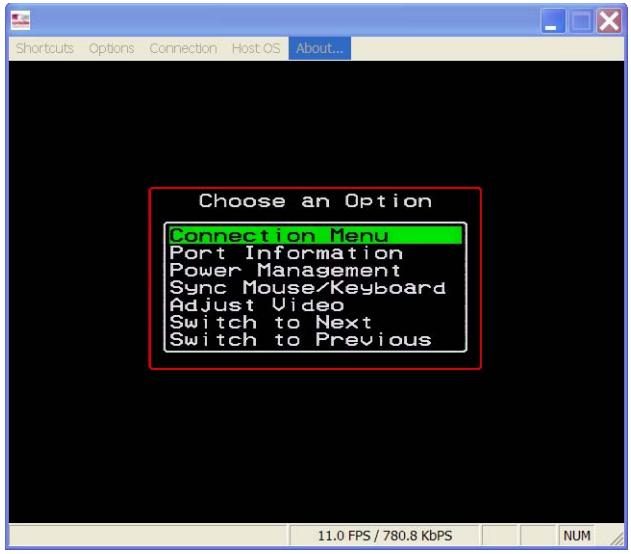


Figure 2-3: Print Screen Menu

Table 2-6 lists and describes the options on the Print Screen Menu.

Table 2-6: Print Screen Menu Options

Option	Description
Connection Menu	Same as KVM port hot key `Ctrl+k q` (see Table 2-7).
Port Information	View the status of the current connection
Power Management	Same as KVM port hot key `Ctrl+k p` (see Table 2-7).

Table 2-6: Print Screen Menu Options (Continued)

Option	Description
Sync Mouse/Keyboard	Same as KVM port hot key `Ctrl+k s` (see Table 2-7).
Adjust Video	Same as KVM port hot key `Ctrl+k v` (see Table 2-7).
Switch to Next	Same as KVM port hot key `Ctrl+k .` (see Table 2-7).
Switch to Previous	Same as KVM port hot key `Ctrl+k ,` (see Table 2-7).

KVM Port Shortcut Hot Keys

The default KVM port shortcut hot keys are described in the following table. These keys are always available for users connected to the OSD through a Local User station, but they are not always available with the AlterPath Viewer. See Table 2-5, “Show Connections Dialog Availability in OnSite Hardware Versions,” on page 84 for information about when they are available in the AlterPath Viewer.

A plus (+) between two keys indicates that both keys must be pressed at once. When two keys are separated by a space, each key must be pressed separately. For example, `Ctrl+k p` means to press the `Ctrl` and `k` keys together followed by the `p` key.

Table 2-7: Default KVM Port Connection Hot Keys

Key Combination	Action
`Ctrl+k q`	Quit. When you are connected to a server through a KVM port and you enter this hot key, the Connection Menu screen appears and you can select another port.  See “To Return to Previous Menus or to Exit” on page 96. for details about the Connection Menu, see “Connection Menu” on page 90.

Table 2-7: Default KVM Port Connection Hot Keys (Continued)

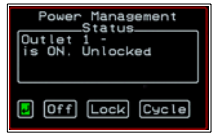
Key Combination	Action
`Ctrl+k p`	Power management. Brings up the Power Management screen with the options to turn on, off, or cycle the power for outlets to which the current server is connected.  **Note:**Cycling is only available for local users through the OSD. See “To Power On, Off, or Cycle a Server While Connected to a KVM Port” on page 100 for the procedure.
`Ctrl+k .`	Next port. Goes to the next authorized port. See “To Connect to the Next Authorized KVM Port” on page 98.
`Ctrl+k ,`	Previous port. Returns to the previous authorized port. See “To Connect to the Previous KVM Port from the Current KVM Port” on page 98.
`Ctrl+k v`	Video. Brings up the “Automatic control” screen with the option to go to the “Manual control” screen.   “Automatic control” lets you set an adjustment value to compensate for the length of the cable running from the OnSite to the KVM terminator that is connected to the server. “Manual control” lets you manually adjust screen brightness and contrast. See “To Adjust Brightness and Cable Length in the AlterPath Viewer” on page 98.

Table 2-7: Default KVM Port Connection Hot Keys (Continued)

Key Combination	Action
`Ctrl+k s`	Reset keyboard and mouse. Brings up a Keyboard Reset screen.  Allows you to reset the keyboard and mouse if the server stops responding to input. See “To Reset the Keyboard and Mouse in the AlterPath Viewer” on page 99.

The OnSite administrator may redefine the KVM port connection hot keys, as described in “Configuring Keyboard Shortcuts (Hot Keys)” on page 63. If the defaults shown in the previous table do not work, check with your OnSite administrator for the site-specified keys to use.

Note: You can use the escape (Esc) key to exit from a screen or viewer.

Sun Keyboard Emulation Hot Keys

A default set of hot keys for emulating Sun keyboard keys is available for use while connected to Sun servers through KVM ports. You can use the Sun hot keys to emulate keys that are present on Sun keyboards but are not present on Windows keyboards.

The hot keys are made up of an escape key followed by a function key or a key from the numeric keypad. The default escape key is the Windows key, which is labeled with the Windows logo. The Windows key usually appears on the Windows keyboard between the `Ctrl` and `Alt` keys.

The following table shows function keys and keys from the numeric keypad that emulate Sun keys when you enter them at the same time as the hot key.

For example, to use the Sun `Find` key, you would press the Windows key at the same time you press the `F9` function key.

Table 2-8: Default Sun Key Emulation Hot Keys

	Win Key	Sun Key
Function Keys	`F2`	`Again`
	`F3`	`Props`
	`F4`	`Undo`
	`F5`	`Front`
	`F6`	`Copy`
	`F7`	`Open`
	`F8`	`Paste`
	`F9`	`Find`
	`F10`	`Cut`
	`F11`	`Help`
	`F12`	`Mute`
Numeric Keypad Keys	`*`	`Compose`
	`+`	`Vol +`
	`-`	`Vol -`

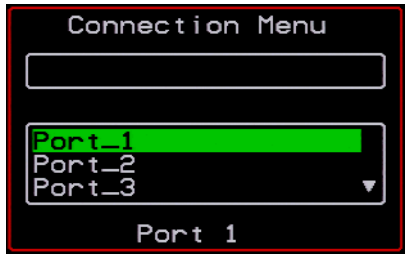
OnSite administrators can change the default escape key portion of the Sun keyboard emulation hot keys from the Windows key to any of the following: `Ctrl`, `Shift`, or `Alt`. See “Configuring Sun Keyboard Equivalent Hot Keys” on page 64 for details and links to procedures.

Connection Menu

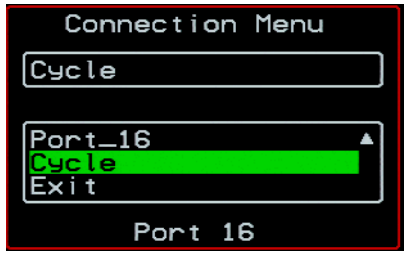
The Connection Menu appears in the following cases:

- When an OnSite administrator selects “Connect” from the OSD Main Menu
- When a regular user logs into the OSD
- When anyone who is connected to a KVM port enters the quit hot key sequence (see Table 2-7 on page 86)

For an administrative user, the Connection Menu lists all the KVM ports. For a regular user, the Connection Menu displays only the KVM ports the user is authorized to access. The KVM ports are listed alphabetically by their default port numbers or administrator-defined aliases, as shown in the following screen example.



The Connection Menu includes the Exit option. For administrative users and for regular users who are authorized for two or more KVM ports, the Cycle option also appears. Both the Exit and Cycle options are shown in the following screen example.



You have two options for selecting KVM ports:

- Scroll down using the arrow keys.

  - OR -

- Type one or more keys that uniquely identify an option if it is not visible in the screen, and then press Enter to complete the name in the text field.

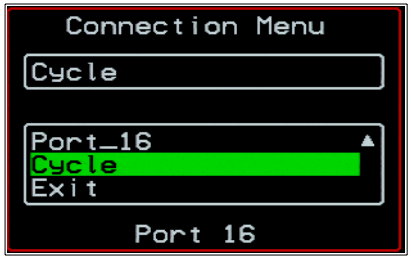
  For example, if you type “c” in the text field, pressing Enter completes the word “Cycle” in the field. You press Enter after choosing the Cycle option to start cycling.

Cycling Among KVM Ports in the OSD

Cycling enables users to view a series of servers connected to KVM ports that the users are authorized to view.

Using the Cycle Option on the Connection Menu

Local OSD users can start cycling among servers using the Cycle option on the Connection Menu. Cycling is only available on the Connection Menu for local users through the OSD.

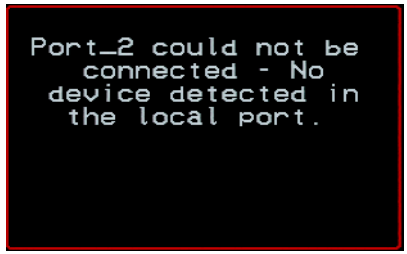


Cycling starts with a view of the server connected to the first port on the Connection Menu list and continues in the order in which the ports are listed until all servers are viewed, and then the cycle starts over again at the beginning. The cycle continues until the user enters the quit hot key (default: `Ctrl+k q`) to return to the Connection Menu.

See “To Cycle Through All Authorized KVM Ports” on page 97.

Administrative users can change the period of time for viewing each server during a cycle. (See “To Configure Local User Sessions [Expert]” on page 221 (Web Manager) and Table 7-15, “KVM Port Configuration Screens [OSD],” on page 437 for how to change the cycle duration.)

If no device is attached to one of the KVM ports that the user has permission to view, a message appears like the following.



Cycle Using a Hot Key Sequence

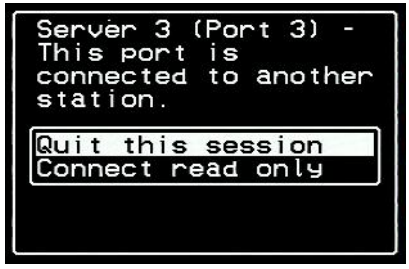
Users can use hot keys to move from viewing one server to another while connected to a KVM port either through the OSD or the Web Manager. See “To Connect to the Next Authorized KVM Port” on page 98 and “To Connect to the Previous KVM Port from the Current KVM Port” on page 98.

Sharing KVM Port Connections

Two authorized users can connect simultaneously to a single KVM port. When the first user is in read-only mode, the new user is always granted the highest level of access for which the new user is authorized. Once two users are connected to a KVM port, either user may choose at any time to change the access mode or disconnect from the session by issuing a hot key or Esc.

KVM Port Sharing Menu Options

When a user connects to a KVM port that is already in use, a screen with a menu of two or more options appears. The following figure shows two options that are always on the menu.



Quit this session

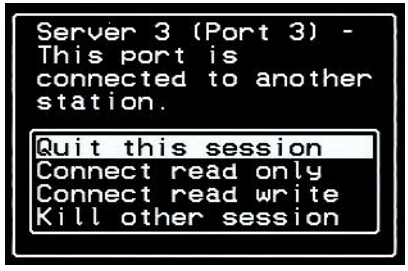
Ends the connection attempt and returns the user to the Connection Menu.

Connect read only

Connects the user in read-only mode and sends this notice to the current user:

User Has Read-Write or Full Access Permissions

If the connecting user has either read-write, or full access permissions for the KVM port, additional menu options appear, as shown in the following figure.



Connect read-write

Connects the new user in read-write mode and sends the notice in the following figure to the current user.

Kill other session

Kills the existing session and connects the new user in read-write mode. Sends the following notice to the current user and disconnects that user:

See “To Share a KVM Port Connection” on page 97 for the procedure.

Common Procedures for Accessing KVM Ports

The following table lists the procedures that can be performed by both OnSite administrators and authorized users while connected to KVM ports, and it provides links to where the procedures are documented.

Table 2-9: Common Procedures While Connected to KVM Ports

Table 2-9: Common Procedures While Connected to KVM Ports

▼ *To Log Into a Server Connected to a KVM Port*

Perform this procedure to log into a server connected to a KVM port either through the Web Manager or through the OSD.

1. Connect to the KVM port.
   a. If using the Web Manager, log in and connect to the KVM port using an option that is available to you.

      See “KVM Port Connection Options” on page 130 for the available options, if needed.

   b. If using the OSD, perform the following steps.

      i. Log into the OSD.

      See “To Log Into the OSD” on page 380 if needed.

      ii. Connect to the KVM port through the Connection menu.

      See “To Select a Server From the Connection Menu” on page 96 if needed.

   If no other user is connected to the port, the connected server’s login prompt or a login dialog box appears.

   If another user is connected to the port, a screen appears with this notice: “This port is connected to another station” and presents two or more options. See “To Share a KVM Port Connection” on page 97 for the options.

2. Log into the server using the username and password supplied by your system administrator.

The procedures for navigating among KVM ports are the same whether you connected to the port through the OSD or the Web Manager. See Table 2-9, “Common Procedures While Connected to KVM Ports,” on page 94 for procedures.

▼ To Select a Server From the Connection Menu

This procedure assumes you have accessed the Connection Menu screen, either through the OSD or through entering the hot key in an AlterPath Viewer. See “To Log Into a Server Connected to a KVM Port” on page 95 for more details.

1. To select a KVM port, do one of the following:

   - Type the first letters of the port name until the desired port is highlighted in the port selection field.

Note: The port name field is case-sensitive.

   OR

   - Select the desired port name from the list.

2. Click “Enter.”

   If no other user is connected to the port, the connected server’s login prompt or a login dialog box appears, unless you have a previous login session in effect.

   See Table 2-9, “Common Procedures While Connected to KVM Ports,” on page 94 for a list of procedures that can be performed while connected to a device.

▼ To Return to Previous Menus or to Exit

This procedure assumes you have connected to a KVM port either through the OSD or through entering the hot key in an AlterPath Viewer.

- Enter the quit hot key (default is `Ctrl+k q`), select the “Exit” option from the current menu (if that option is available), or press the `Esc` key.

▼ To Share a KVM Port Connection

Follow this procedure after connecting to a KVM port (as described in "To Log Into a Server Connected to a KVM Port" on page 95), if you find that another user is already connected to the same KVM port. A screen appears with the notice: "This port is connected to another station" and presents two or more options. See "Sharing KVM Port Connections" on page 92 for details about the notification screens, if needed.

1. To connect to the server in "read-only" mode, select "Connect read-only."

   The other user is notified of the new connection.

2. To connect to the server in "read-write" mode and notify the other user, select "Connect read write."

   If the other user is connected in "read-write" mode, the other user's access mode is changed to "read-only", and the user is notified of the change.

3. To kill the existing session and connect in "read-write" mode, select "Kill the other session."

   The other user receives a notice and is disconnected from the KVM port.

   AlterPath viewer displays whatever you would see if you were directly logged into the connected server.

▼ To Cycle Through All Authorized KVM Ports

You can perform this procedure if you are authorized for two or more KVM ports. See "Cycling Among KVM Ports in the OSD" on page 91 for details, if needed.

1. Bring up the Connection Menu by doing one of the following actions.

   a. Log into the OSD and choose Connect from the Main Menu.

      See "To Log Into the OSD" on page 380, if needed.

   b. If you are already connected to a port, enter the quit hot key (default=`Ctrl+k q`).

   The Connection Menu appears.

2. Choose "Cycle."

a. If the “Cycle” option is not visible, type the letter c in the field and press Enter to highlight the Cycle option.

b. Click “Enter” to select the “Cycle” option.

The Server Selection Menu appears.

3. To abort the process and close the session, enter the quit hot key again.

▼ To Connect to the Next Authorized KVM Port

While you are connected to a server through a KVM port, do the following to connect to another server you have permission to access. See “To Log Into a Server Connected to a KVM Port” on page 95 and “Cycling Among KVM Ports in the OSD” on page 91, for more information if needed.

- Use the Next keyboard shortcut (default=`Ctrl+k .`).

  The next authorized server appears. Repeat this step to move to the next server.

▼ To Connect to the Previous KVM Port from the Current KVM Port

While you are connected to a server through a KVM port you can do the following to connect to another server you have previously accessed. See “To Log Into a Server Connected to a KVM Port” on page 95, for more information if needed.

- Use the Previous keyboard shortcut (default=`Ctrl+k ,,`).

  The previous server appears. Repeat this step as needed to move to other previous servers.

▼ To Adjust Brightness and Cable Length in the AlterPath Viewer

Perform this procedure to adjust the screen brightness and to adjust for varying cable lengths. See Table 2-7, “Default KVM Port Connection Hot Keys,” on page 86 for details about the video control screens, if needed.

- You can adjust the brightness on the “Manual control” screen “Brightness” scale.

  The higher the value, the greater the brightness.

- You can adjust for varying cable lengths on the following screens:
  - On Automatic control screen's "Adjustment" scale
  - On the Manual control screen "Cbl Len Adj" scale.

  Chose lower values for longer cables. For example, for a 500-foot cable, the setting might be 10 or 20. For a shorter cable of 6 or 3 feet, a value of 128 or 150 is more appropriate. The correct setting can avoid poor video quality.

1. Enter the video control keyboard shortcut (default=`Ctrl+k v`).

   Depending on which screen was accessed last, one of the following screens appears.

   - Automatic Control
   - Manual Control

2. To switch to the Automatic control screen or the Manual control screen select Auto or Manual respectively.
3. To compensate for differing cable lengths, do one of the following:

   a. On the Automatic Control screen, press the right or left arrows to set the desired value in the "Adjustment" scale.

   b. On the Manual Control screen, press the right or left arrows to set On the desired value in the "Cbl Len Adj" scale.

4. To adjust screen brightness on the Manual Control screen, press the right or left arrows to set the desired value in the "Brightness" scale.

▼ *To Reset the Keyboard and Mouse in the AlterPath Viewer*

Do this procedure if the server stops accepting keyboard and mouse input that you are entering in the AlterPath Viewer.

1. Use the keyboard/mouse reset hot key (default=`Ctrl+k s`).

   The confirmation screen appears.

2. Select Yes.

   See "KVM Port Access Requirements" in the *AlterPath OnSite Installation Guide* for information on avoiding problems using the mouse.

▼ To Power On, Off, or Cycle a Server While Connected to a KVM Port

This procedure assumes the prerequisites in “Power Management” on page 76 are complete. The default power management hot key sequence is: `Ctrl+k p`. Power management while connected is the same whether the KVM port connection was made through the OSD or the Web Manager.

1. Log into the OnSite, connect to the port, and log into the server.

- See “To Log Into a Server Connected to a KVM Port” on page 95, if needed, for how to log in through the Web Manager. You can access a KVM port through the OSD connect menu, but regular users should usually connect to both KVM and serial ports through the Web Manager.

2. Make sure the AlterPath viewer is active, and then enter the hot key.

   The Power Management screen displays with a list of the outlets that are configured for the server that is connected to this KVM port.

3. Type the power management keyboard shortcut.

   The Power Management screen appears.

4. Select an outlet.

5. Do one of the following:

   - To turn the power on, select “On.”
   - To turn the power off, select “Off.”
   - To turn the power off briefly and then on again, select “Cycle.”
   - To lock the selected outlet, select “Lock.”
   - To unlock the selected outlet, select “Unlock.”

▼ To View Information About a KVM Port While Connected

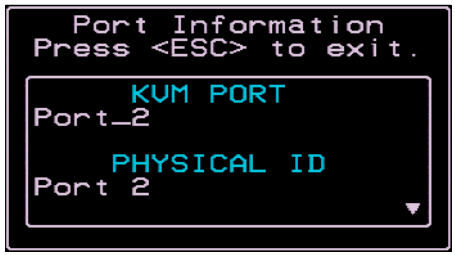
Follow this procedure to view the alias (if defined) and the port number for a port while connected. An administratively-assigned alias often is used to identify the server that is connected to the port.

1. Connect to the server.

See “To Log Into a Server Connected to a KVM Port” on page 95, if needed.

2. Use the information hot key (default=`Ctrl+k i`).

   The following screen appears.



3. Click “Esc” to exit the KVM Port Information screen and return to the connected server.

Serial Port Connections

A serial port may be connected to the following two types of devices:

- A headless server or other device that has a console port.

  This is the most common use of a serial port. An authorized user or administrator can then make a `telnet` or `ssh` or raw socket connection to the port through the OnSite, and then log into the device that is connected to the port.

- A dumb terminal

  The dumb terminal may be configured to be able to access only a single server or it may be able to access multiple servers. The OnSite administrator can configure either of the two following actions to occur when the terminal is turned:

  - A `telnet`, `ssh`, or raw socket connection is made to a single remote server

    - OR -

  - A menu is presented with options for connecting to remote servers.

When a Dumb Terminal is Connected to a Serial Port

If the dumb terminal is configured as a dedicated terminal, a session starts up on the designated server with the administratively-defined connection protocol. For example, if the administrator has assigned the Telnet protocol when configuring the dumb terminal's serial port, a viewer launches running a `telnet` session on the console of the specified server.

If the dumb terminal is configured as a local terminal with access to the OnSite, either of the two following options appears:

- A login prompt

  This connection allows you to log into the OnSite on the command line. If you are authorized to log in as root, you can run any commands recognized by the Linux operating system.

- A menu of connection options

  The menu can be configured by the local administrator and usually has multiple options for launching SSH sessions on remote hosts. For example, the following menu called "SSH to Servers" lists options that launch `ssh` connections to several servers, such as shown in the following screen example.

```
SSH_to_Servers
==============

SunServer1_CA

WinXPServer_BR

WindowsMEServer_NY
```

▼ To Connect Through a Dumb Terminal to a Server or to the OnSite

This procedure assumes that a dumb terminal is connected to one of the OnSite's serial ports and that the terminal is configured either as a dedicated terminal for making a `telnet` or `ssh` connection to a server or as a local terminal for connecting to the OnSite.

1. Turn on the terminal.

   If the dumb terminal is configured as a dedicated terminal, a session with the administratively-defined connection protocol starts up on the server. If the dumb terminal is configured as a local terminal with access to the OnSite, either of the two following appears:

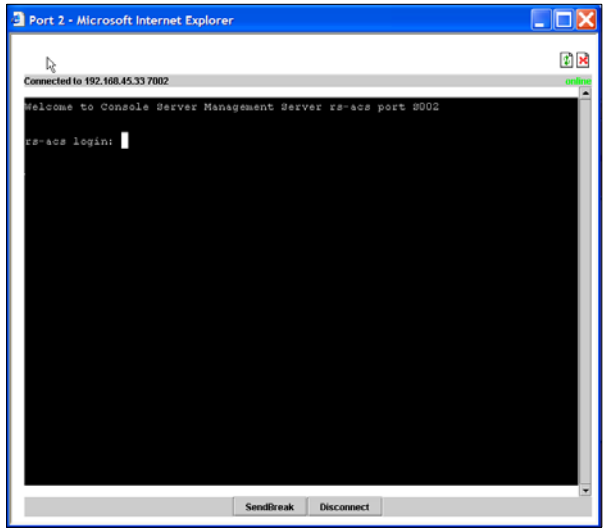
   - A login prompt that allows you to log into the OnSite as root on the command line and run the *CLI* or any other commands recognized by the Linux operating system.
   - A menu of connection options.

2. If presented with a login prompt, log in.
3. If presented with a menu of options, select the desired option.

Connecting to Serial Ports

Connecting to a serial port through the Web Manager or through `telnet` or `ssh` brings up a Java applet with a connection to the attached device's console port. Logins persist across connection sessions. If you close a connection without logging out, you will still be logged in the next time you connect, unless the device has closed your session. If you are not currently logged in, you see a login prompt.

The following figure shows a login prompt.



The Java applet viewer shows the serial port number or administratively-defined alias. The message at the top of the screen shows the IP address of the OnSite followed by the TCP port number. In the previous screen example, the IP address is `192.168.45.33` and the TCP port number is `7002` (the default TCP port number for serial "Port 2").

You can send a break to a server using the SendBreak button and disconnect from the device using the "Disconnect" button.

Hot Keys for Serial Port Connections

The default IPDU power management hot key is `Ctrl+p`. The default IPMI power management hot key is `Ctrl+Shift+i`.

Connection Protocols for Serial Ports

You can access the console of a device connected to a serial port by using the connection protocol specified for the port. The following list shows all the protocols the OnSite administrator can choose for console logins through serial ports:

- `telnet`
- SSHv1
- SSHv2

Ask your OnSite administrator for the connection protocol that you should use if the default `telnet` does not work.

TCP Port Numbers for Serial Ports

The TCP port numbers by default are 7001 through 7008. TCP port number 3000 refers to a pool of all serial ports. The OnSite administrator may change the default port numbers, so if you use the defaults and they fail, check with the administrator to find which port numbers to use.

▼ To Use Telnet to Connect to a Device Through a Serial Port

For this procedure, you need the hostname of the OnSite or its IP address and the TCP port number for the serial port to which the device is connected. See "TCP Port Numbers for Serial Ports" on page 104 if needed.

1. To use `telnet` on the command line in a shell, enter the following command:

```
telnet hostname|IP_address TCP_port_number
```

2. To use `telnet` in a terminal emulation program that provides a telnet client, enter the IP address in the destination field and the TCP port number in the port field.

▼ To Use SSH to Connect to a Device Through a Serial Port

For this procedure, you need the hostname of the OnSite or its IP address and the TCP port number for the serial port. See "TCP Port Numbers for Serial Ports" on page 104 if needed.

1. To use `ssh` in a shell, enter the following command:

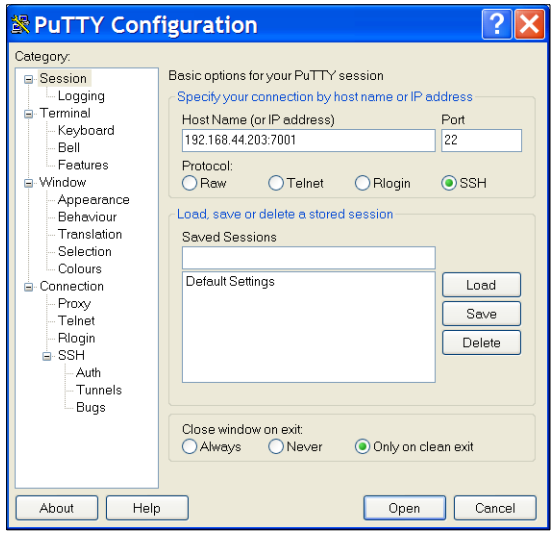
```
ssh -l username:TCP_port_number OnSite_IP_address
```

   For example, to login into the device connected to port 1 on an OnSite whose IP address is 192.168.44.203, you would enter the command shown in the following screen example.

```
ssh -l admin:7001 192.168.44.203
```

2. To use `ssh` in an SSH client application, enter the IP address followed by a colon (:) followed by the port number in the destination field.

   The ssh application supplies the default SSH port number in the Port field as shown in the following screen example.



The `ssh` session is started on the connected device's console port and the login prompt or dialog box appears, as shown in the following screen example.

3. Login using the appropriate login name for the type of work you are authorized to do on the port.

▼ To Log Into a Device's Console Through a Serial Port

See "Serial Port Connections" on page 101 for background information, if needed.Selecting a port number or alias and

1. Connect to the port.
   a. To connect to the serial port through the Web Manager, do the following steps.
      i. Log into the Web Manager.

      If needed, see "To Log Into the Web Manager" on page 128.

      ii. Select the serial port number or alias from the pull-down menu on the "Connect to Server" screen.

      iii. Click the Connect button.

      If needed, see "Connect to Server>Connect to Serial Ports" on page 144.

   b. To connect to the serial port through `telnet`, `ssh`, or a raw device connection, do the following steps.
      i. Launch the connection application.

      ii. Enter the OnSite's IP address and the TCP port number of the serial port.

      See "To Use Telnet to Connect to a Device Through a Serial Port" on page 104 or "To Use SSH to Connect to a Device Through a Serial Port" on page 105, if needed.

   A Java applet appears connected to the console of the device that is connected to the serial port.
2. Enter the required name and password to log into the console of the connected device.

▼ To Manage Power While Connected to a Serial Port

1. Log into the OnSite, connect to the serial port, and log into the device, if needed.

See “To Log Into a Device’s Console Through a Serial Port” on page 107, if needed.

The Java applet appears.

2. Enter the hot key to bring up the power management menu.

   `Ctrl+p` is the default IPDU power management hot key.
   `Ctrl+Shift+i` is the default IPMI power management hot key.

   If you do not have any power management permissions, the following message appears.

> It was impossible to start a Power Management Session.
>
> You cannot access any Power Management functionality.
>
> Please contact your Console Server Administrator.

   If you do not have permission to manage power for the server connected to this serial port, the following message appears.

> You cannot manage the outlet(s) of this server.
>
> Please enter the outlet(s) (or ‘h’ for help):

   If you have permission to perform IPDU power management on this serial port, the IPDU power management menu displays as shown in the following screen example. The first line shows the number of the first outlet you have permission to manage through the serial port.

```
IPDU a1 Outlet 8:
------------------------------------------------
  Cyclades Corporation - Power Management Utility
------------------------------------------------
   1 - Exit          2 - Help        3 - On
   4 - Off          5 - Cycle       6 - Lock
   7 - Unlock        8 - Status      9 - Interval
   10 - Other

Please choose an option:
```

If you have permission to perform IPMI power management while connected to this serial port, the following menu appears.

```
------------------------------------------------
    Cyclades Corporation - IPMI Power Management
------------------------------------------------
 1 - Exit         2 - Help         3 - On
 4 - Off          5 - Cycle       6 - Status

Please choose an option:
```

3. To exit from the power management session, do one of the following:

- **a.** Enter the hot key (default `Ctrl+q`) any time.
- **b.** If the “Please choose an option” prompt is waiting, type option “1.”
- **c.** If the prompt “Please enter the outlet(s) ...” is waiting, type “T.”

The following message appears.

```
Exit from PM session
```

▼ To Use ts_menu to Connect to a Serial Port

1. Log into the OnSite in one of the following ways.
   a. Log in as "root" locally through the console port.
   b. Log in as "root" by using `telnet` or `ssh`.
      i. Make sure the port is configured for the connection protocol you want to use.

      See "To Configure Serial Ports [Wizard]" on page 174 or "To Configure a Serial Port Connection Protocol for a Console Connection [Expert]" on page 236 for how the connection protocol is specified for a serial port, if needed.

      ii. If you are using `telnet`, configure an escape character to use for ending the telnet session later.

      Because the default `ts_menu` escape character for telnet sessions is `^]` (caret and right bracket), you need to configure a different escape character for `telnet` at this time. Otherwise, using `^]` to exit the serial port console session created through `ts_menu` also closes the `telnet` session on the OnSite.

      If using `telnet` on the command line, you can use the `-e` option in the format shown in the following screen example.

      ```
      # telnet -e ^X OnSite_IP_address
      ```

      The following example shows the `telnet` command used to set `Ctrl+?` as the escape character and to connect to an OnSite whose IP address is `192.168.160.10`.

      ```
      # telnet -e ^? 192.168.160.10
      ```

   c. Log in as "admin" through the Web Manager

      See "To Connect to the OnSite Console as admin [Expert]" on page 193, if needed.

2. Enter the `ts_menu` command at the prompt.

```
[root@rskvm root]# ts_menu
```

The `ts_menu` displays a numbered list of all the serial ports you are authorized to access showing their device names or any aliases configured for the ports, as in the following example.

```
Serial Console Server Connection Menu for your Master Terminal Server


1 ttyS1 2 ttyS2 3 ttyS3 4 ttyS4

5 ttyS5 6 ttyS6 7 ttyS7 8 ttyS8


Type 'q' to quit, a valid option[1-8], or anything else to refresh:
```

3. Enter the number that corresponds to the serial port you want to access.

The following screen example shows the number 1 entered to access port ID `ttyS1`.

```
Type 'q' to quit, a valid option[1-8], or anything else to refresh: 1
```

`ts_menu` makes a console connection to the specified port and displays a prompt. The following example shows the prompt when the serial port 1 is configured for power management.

```
------------------------------------------------------------------------

Cyclades Corporation

Power Management Command Prompt v1.1

------------------------------------------------------------------------

Power Name: ttyS1


[ttyS1]
```

Dial-in Connections

"Dial-in Connections" on page 112 lists the types of devices that can be used for dial-in access to the OnSite.

You use either of the following methods to dial in:

- PPP (when dialing into any of the supported modems)

  Once the connection is made, all requests to access the specified IP address are routed through the PPP connection. For example, if you enter the specified IP address in a browser, the browser connects to the OnSite through the dial-in connection. This way you can access the Web Manager or the OnSite's console through PPP even if the Ethernet connection to the OnSite is not available.

- A terminal emulator (only when dialing into a modem on a PCMCIA card)

  On a computer running a Windows operating system, you can use HyperTerminal or another terminal emulator. On a computer running a UNIX-based operating system, such as Solaris or Linux, you can use a compatible terminal emulator such as Kermit or Minicom.

  Once the dial-in connection is made using a terminal emulator, you get console access to the OnSite.

The OnSite administrator performs the procedures to install and configure the modems. Contact your OnSite administrator for the phone numbers, usernames, and passwords to use, and for questions about how the modems are configured.

The parameters for the PPP connection can be configured on the remote computer and saved in a list of connection profiles by name. Subsequently, users can click on a desired connection name to dial in without having to enter the parameters each time. For example, if you want to contact the modem of an OnSite located in Massachusetts to set up a callback session, you might name the connection, "OnSiteMAcallback." Later, if you want to dial into the OnSite in Massachusetts, you can click the OnSiteMAcallback connection name to create the connection automatically.

Before configuring PPP, you need the following:

- A modem connected to your computer.
- The phone number of the line that is dedicated to the OnSite modem you want to access.
- If authentication is required for the device into which you dial, you need a username and password for a user account on the OnSite.

The following table lists the related procedures and where they are documented.

Table 2-10: Tasks for Configuring and Making Dial-in Connections

Task	Where Documented
Configure a PPP connection profile with stored phone number, user, and password information	"To Configure a Reusable PPP Connection" on page 114
Connect using a preconfigured PPP connection profile	"To Start a PPP Connection From a Remote Computer" on page 115
Configure a terminal connection profile with stored phone number, user, and password information	"To Configure a Reusable Terminal Emulator Dial-in Connection" on page 116
Connect using a stored terminal emulator connection profile	"To Dial Into the OnSite Using a Terminal Emulator" on page 117
	"To Dial Into the OnSite Using a Terminal Emulator" on page 117

▼ *To Configure a Reusable PPP Connection*

Perform this procedure on a remote computer with a modem to do the following:

- Assign a name and define the parameters for a PPP connection profile that can be re-used for dialing into the OnSite.

  Defining a reusable "connection" with a name and the desired parameters saves users the trouble of entering the phone number, username, and password every time they want to dial into the OnSite.
- Optionally configure callback.
- Optionally dial-into the OnSite.

See the prerequisites listed in "Dial-in Connections" on page 112, if needed.

Note: The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems. You can use this procedure as an example.

---

1. From "My Computer," go to "My Network Places."
2. Under "Network Tasks," click "View network connections."
3. Under "Network Tasks," select "Create a new connection."

   The "New Connection Wizard" appears.
4. Click the "Next" button.
5. Click "Connect to the Internet" and click "Next>."

   The "Getting Ready" screen appears.
6. Click "Set up my connection manually" and click "Next>."

   The "Internet Connection" screen appears.
7. Click "Connect using a dial-up modem" and click "Next>."

   The "Connection Name" screen appears.

   Type a name for the connection in the "ISP Name" field and click "Next>."

   The "Phone Number to Dial" screen appears.

8. Type the phone number for the OnSite's modem in the "Phone number" field and click "Next>."

   The "Internet Account Information" screen appears.

9. Type the username for accessing the OnSite in the "User name" field.

10. Type the password for accessing the OnSite in the "Password" and "Confirm Password" field and click "Next>."

11. Click the "Finish" button.

    The "Connect *connection_name*" dialog appears.

12. Click the "Cancel" button.

    The name of the connection appears on the Network Connections" list.

13. To configure call back, do the following steps.

    a. Select the name of the connection from the Network Connections dialog box.

    b. Select "Dial Up Preferences" from the "Advanced" menu.

       The "Dial-up Preferences" dialog box appears.

    c. Click the "Callback" tab.

    d. Click "Always call me back at the number(s) below."

    e. Highlight the name of the modem and click "Edit."

       The "Call Me Back At" dialog box appears.

    f. Enter the phone number of your local modem in the "Phone number:" field, and click OK.

▼ *To Start a PPP Connection From a Remote Computer*

Perform this procedure on a remote computer that has a modem to initialize a dial-in and optional call back session on the OnSite. This procedure assumes a PPP connection profile has previously been configured with the modem or phone card's phone number, username, and password, as described in "To Configure a Reusable PPP Connection" on page 114.

Note: The following steps work if you are on a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use these steps as an example.

1. From the Start menu, go to My Computer>My Network Places.
2. Under “Network Tasks,” click “View network connections.”
3. Double-click the name of the connection in the list.

   The “Connect *connection_name*” dialog appears. The stored username and password appear in the “User Name” and “Password” fields and the phone number appears in the “Dial” field.
4. Click the “Dial” button.

   If the OnSite administrator has configured the modem or phone card for authentication, then you are prompted for your username and password.
5. Log in with your username and password if prompted.

▼ *To Configure a Reusable Terminal Emulator Dial-in Connection*

Do this procedure on a remote computer that has a modem to assign a name and configure parameters for a named connection profile. This procedure can only be used for dialing into a modem that is on a PCMCIA card on the OnSite. See the prerequisites listed in “Dial-in Connections” on page 112, if needed.

Note: The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use this procedure as an example.

1. From the Start menu, go to All Programs>Accessories> Communications>Hyperterminal.
2. Select “New Connection” from the “File” menu.
3. Type a name in the “Name” field, select an icon for the connection, and click OK.
4. Enter the phone number assigned to the PCMCIA modem card.

5. Select a country or region from the “Country/region” pull-down menu.
6. Fill in the “Area Code” and “Phone number” fields.
7. Select the modem from the “Connect using” pull-down menu, and click OK.

   The new connection appears in the list of connections appearing on the “Open” menu.

▼ *To Dial Into the OnSite Using a Terminal Emulator*

This procedure requires a PCMCIA modem card installed on the OnSite. If the OnSite administrator has configured the modem card for callback, when you dial in, the OnSite calls back to the specified number. Contact your OnSite administrator if you have questions about the configuration. This procedure also assumes that a previously-defined connection is listed in the terminal emulator’s list of connections, as described in “To Configure a Reusable Terminal Emulator Dial-in Connection” on page 116.

Note: The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use this procedure as an example.

---

1. From the Start menu, go to All Programs>Accessories>Communications>Hyperterminal>*connection_name*.

   For example, a previously-configured connection named “dial_onsite” appears in the HyperTerminal Open list as “dial_onsite.ht.”

   If the OnSite administrator has configured the PCMCIA modem card for callback, when you dial in, the OnSite calls you back and prompts you for a user name.

   .If the OnSite administrator has configured the modem or phone card for OTP (one time password) authentication, then you are prompted for your OTP username and OTP password.

2. Log in with your username and OTP password if prompted.

   See “To Generate an OTP Password When Challenged at Dial-in” on page 119, if needed.

3. If call back is enabled, enter **`cbuser`** at the user name prompt.

Obtaining and Using One Time Passwords for Dial-ins

This section is for users who are authorized to dial into the OnSite through a modem or phone PCMCIA card if the *one time password* (OTP) authentication method is configured for dial-ins to that device. If you are not sure, ask your OnSite administrator.

If the OTP authentication method is in effect for dial-ins to a modem or phone card, you need to supply a different password whenever you dial-in. Because OTP passwords are different every time, no one who discovers the password that you use for one session can use that password later to connect to your account.

A one time password is actually a group of six English words (for example: `GOLD ARK FISH DOVE SON ZION`) that are entered all on the same line at the prompt. You might be given a series of one time passwords; following is an example sequence:

```
495: AMEN FONT STAR SEA WINE RED
496: ART LILY HOLY AID LOVE ALL
497: GOLD ARK FISH DOVE SON ZION
498: SEE PITY JOY HOPE PLAN CITY
```

At the first login, you would enter the password from line 498, on the next login, you would enter line 497, and so forth.

Each user who needs to use OTP needs a local user account on the OnSite, must be registered with the OTP system, and must be able to obtain the OTP username, OTP secret pass phrase, and OTP passwords needed for logins. See the following list for how the OnSite administrator may register and give OTP passwords to users:

- Register all users and give OTP usernames and OTP secret pass phrases to each user.

  AND

- Generate the needed OTP passwords on behalf of the each user and give them to each user.

Some sites choose to print out hard copy lists of OPIE passwords for their users and deliver them by methods such as FAX or FedEx.

OR

- Make sure users are equipped with an OTP generator that is not on the network to generate their own OTP passwords when challenged at login time.

The OTP generator may be a copy of the `opiekeys` program installed on the user's workstation, or it may be an OTP token card.

▼ To Generate an OTP Password When Challenged at Dial-in

Following is an example procedure for a user who has /etc/`opiekeys` installed on the user's workstation:

1. Dial into the OnSite through a PCMCIA modem or phone card that has been configured to use OTP authentication.

   The OnSite challenges with a *sequence number* (also called a counter) and a *seed* (or key) associated with the username and asks for a response.

   The seed includes the first two letters of the hostname and a pseudo random number.

```
login: username
otp-md5 499 on93564
Response:
```

   The challenge is `otp-md5 499 on93564`. The sequence number / counter is 499 and the seed is `on93564`.

2. Obtain an OTP password by performing the following steps.

   a. Copy the entire challenge into a window on a computer where the `opiekey` program is installed.

      The `otp-md5` portion of the challenge is a symbolic link to the `opiekey` program and tells the `opiekey` program to use the MD5 algorithm. `opiepasswd` then prompts the user for the user's secret pass phrase.

   b. Enter your secret pass phrase when prompted.

The `opiekey` program generates a six word OTP password, such as `GOLD ARK FISH DOVE SON ZION`.

3. Copy the OTP password to the window where the login program is waiting with the “Response” prompt.

```
Response: GOLD ARK FISH DOVE SON ZION
$
```

The user’s sequence number is decremented in the OnSite-resident opiekeys file.

Managing IPDU Outlets With PM Commands

An OnSite administrator who knows the root password and can access the console of the OnSite can manage power outlets on connected IPDUs from the command line using either the `pm` command or the `pmCommand` command. The following procedure gives an introduction to these commands. Refer to the Cyclades AlterPath PM documentation for more details.

▼ *To Manage IPDUs from the Command Line as Root*

1. Make a local connection to the console port of the OnSite, or use `telnet` or `ssh` to access the OnSite from a remote location, and log in.
2. Enter either the `pm` command or the `pmCommand` command followed by the AUX port number to which the AlterPath PM IPDU is connected.

```
[root@ONS root]# pm port_number
- OR -
[root@ONS root]# pmCommand port_number
```

Use `a1` to specify AUX port 1 and `a2` to specify AUX port 2. For example, to manage power on an IPDU connected to AUX port 1, you would enter the command as shown in the following screen example.

```
[root@ONS root]# pm a1
- OR -
[root@ONS root]# pmCommand a1
```

The `pmCommand` entered alone on the Linux command line displays usage guidelines, as shown in the following screen example.

```
[root@ONS root]# pmCommand
Use: pmCommand <serial port number> <command> <arguments>
where: <serial port number>  is the serial port number
configured as IPDU
       <command> <arguments> are the PM command and its
arguments.
[root@ONS root]#
```

The `pmCommand` entered with a port number displays the menu shown in the following screen example.

```
[root@ONS root]# pmCommand a1
------------------------------------------------------------
Cyclades Corporation
Power Management Command Prompt v1.1
------------------------------------------------------------
Power Name: AuxPort1
Number of units: 1
Aux Port: 1
Type  help  for help
Type  menu  for menu driven interface
Type  exit  to exit
------------------------------------------------------------
[AuxPort1]
```

Typing “help” at the prompt shown in the previous screen example bring up a list of available subcommands shown in the following screen example.

```
[AuxPort1] help
on|off -------------- Turn on|off outlets
lock|unlock --------- Lock|unlock outlets in current state
cycle --------------- Power cycle outlets
interval|buzzer ----- Set/read the power up interval|buzzer
syslog|alarm -------- Set/read syslog notifications|alarm
status
temperature|current - Set/read/reset the temperature|current
currentprotection --- Set/read the over current protection
name ---------------- Name an outlet
status -------------- Display state of the outlets
reboot  ------------- Reboot the units in chain
help ---------------- Show this help
ver ----------------- Show the software and hardware version
whoami -------------- Display the current username
exit ---------------- Exit
menu ---------------- Start the menu driven text interface(pm)
factorydefaults ----- Bring the unit to factory configuration
restore ------------- Restore the configuration in flash
save ---------------- Save the current configuration in flash
```

Entering **menu** at the prompt brings up the same menu as the pm command.

The Power Management menu is shown in the following screen example.

```
------------------------------------------------------------
Cyclades Power Management Menu

PowerPort: AuxPort1
------------------------------------------------------------
1. Exit    7. Status      13. Who Am I            19. Restore
2. On      8. Interval    14. Help                20. Save
3. Off     9. Name        15. Buzzer              21. Syslog
4. Cycle  10. Current     16. Current Protection  22. Alarm
5. Lock   11. Temperature 17. Factory Default
6. Unlock 12. Version     18. Reboot

Please choose an option:
```

3. At the prompt, enter the number that corresponds to the desired option.

Which prompt appears varies according to the selected option. For example, choosing option 4 brings up the prompt shown in the following screen example.

```
Please choose an option: 4
Please enter the outlets (or 'help' for help):
```

When prompted, enter one or more outlet numbers separated by commas or dashes, as shown in the following screen example, or enter "all."

```
Please enter the outlets (or 'help' for help): 1-3, 5
```

4. When you are done, enter 1 to exit.

Chapter 3
Web Manager Introduction

This chapter describes the rules and prerequisites for accessing the Cyclades Web Manager on the OnSite, introduces the Wizard and Expert modes, and describes how to log in.

This chapter also provides important prerequisite information for understanding the information and procedures in the rest of this manual.

The following table lists the topics in this chapter.

Accessing the Web Manager

Both OnSite administrative users and authorized users can access the Web Manager from a browser.

OnSite administrative users who are logging into the Web Manager to perform OnSite configuration and any user logging in to monitor the OnSite's temperature or to perform IPDU power management can use any modern browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla or Firefox).

Browsers used for logging into the Web Manager to access devices connected to KVM or serial ports must meet additional requirements described in "Other Web Manager Login and Port Connection Options and Requirements" on page 129.

Access to the Web Manager is through one of the following ways:

- Through the Ethernet port
- Through a dial-in or callback connection with one of the following:
  - The internal modem
  - An optional external modem connected to the modem port or to one of the AUX ports
  - A modem on an optional PCMCIA modem card

Only one OnSite administrative user can be logged into the Web Manager at a time. If a second administrative user attempts to log into the Web Manager, the prompt shown in the following figure appears.

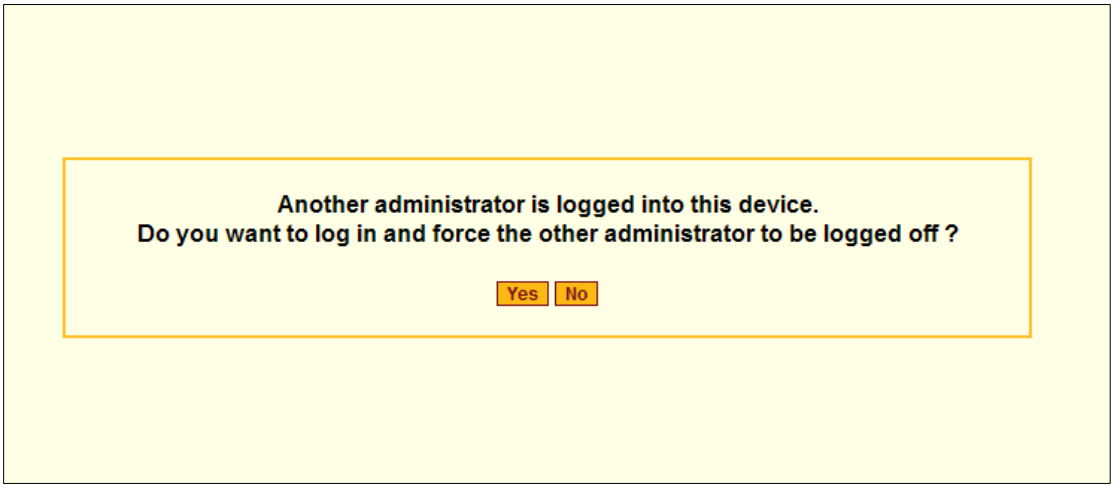


Figure 3-1: Web Manager Prompt When Another Administrative User is Logged In

If the dialog in Figure 3-1 appears, the administrator clicks the “Yes” button to log in and force the other administrative user to be logged out.

Any number of regular users can connect to the Web Manager at the same time.

Prerequisites for Using the Web Manager

The prerequisites describedin this section must be complete before anyone can access the Web Manager. If you have questions about any of the following prerequisites, contact the OnSite’s installer.

- Basic network parameters must be defined on the OnSite so the Web Manager can be launched over the network.

  See the *AlterPath OnSite Installation Guide* for how the installer defines basic network parameters on the OnSite.

- The IP address of the OnSite must be known.

  Entering the IP address of the OnSite in the address field of one of the supported browsers is the first step required to access the Web Manager.

If DHCP is enabled and you do not know how to find out the current IP address of the OnSite, contact the OnSite's installer for help.

- The user account must be defined on OnSite

  By default, the "admin" has an account on the Web Manager. An administrative user can create regular user accounts and authorize them to access connected devices using the Web Manager.

▼ *To Log Into the Web Manager*

1. Enter the IP address of the OnSite in the address (URL) field of a browser.

Note: Check with the administrator who configured the basic network parameters on the OnSite for the IP address and the password, if needed.

   - If DHCP is not enabled, use a static IP address or DNS-administered name assigned by the network administrator to the OnSite.
   - If DHCP is enabled, enter the dynamically-assigned or a fixed IP address defined on the DHCP server.

   The Login screen appears.

2. Enter your account name in the "username" field and the password in the "password" field.
3. Click "Go."
   - For regular users, if the "Web Manager - Regular User" window appears you are finished logging in. See Chapter 4, "Web Manager for Regular Users," if needed, for how to use the Web Manager after logging in.
   - For administrative users, the Web Manager comes up in one of two modes.

     See "Web Manager Modes" on page 135, if needed, for an introduction to the modes.

     - The first time the admin user logs in, the Web Manager Wizard mode automatically comes up at "Step 1: Security Profile" to prompt the admin user to select a security profile before continuing to perform the other Wizard steps.

See Chapter 5, “Web Manager Wizard Mode,” for how to perform configuration in Wizard mode.

- At all other logins by administrative users, Web Manager Expert mode is the default mode.

  See Chapter 6, “Web Manager for Administrators,” for how to perform configuration in Expert mode.

- If another administrator is already logged in as “admin,” a dialog box appears.

4. If a dialog prompts you to verify whether you want to proceed by logging the other admin out or by cancelling your login attempt, enter “Yes” to log in.

Other Web Manager Login and Port Connection Options and Requirements

All types of users who need to connect KVM or serial ports need a supported and configured browser, as described in the *AlterPath OnSite Installation Guide*. Following is a partial list of the requirements described in the installation guide.

- For access to KVM ports through the Web Manager, which brings up an AlterPath Viewer, the browser must have the Active X plug-in enabled and must be running on a Windows computer with the specified minimum configuration.
- Mouse settings on a server that is connected to a KVM port must be configured properly or the user’s mouse cannot track over the KVM connection.
- For access to serial ports through the Web Manager, which brings up a Java applet, the Java Runtime Environment (JRE) 1.4.2 or later version must be installed on your computer and the Java plug-in must be installed in the browser to support the Java applet through which the serial port connection is made.

Following sections describe options for connecting to servers connected to KVM ports and devices connected to serial ports.

KVM Port Connection Options

This section describes the different ways that OnSite administrators and authorized users access servers connected to KVM ports through the Web Manager. The two options listed below depend on whether or not direct access to KVM ports is enabled as described in “Direct Access to KVM Ports and KVM Port Authentication” on page 45:

- If direct access to KVM ports is not enabled, users can access servers connected to KVM ports after first logging into the Web Manager, and then connecting to the KVM port from the Connect to Server screen.
- If direct access to KVM ports is enabled, administrative users and authorized users can access KVM ports through the Web Manager login screen.

Connecting to KVM Ports When Direct Access is Disabled

- Table 3-1 gives the sequence for how you can log into a server connected to a KVM port through the Web Manager *when direct access to KVM ports is not enabled*.

Table 3-1: Connecting to KVM Ports Via Web Manager When Direct Access is not Enabled

Login Sequence	Where Documented
1. You enter the OnSite’s IP address or DNS name in a browser to bring up the Web Manager login screen, and you log into the Web Manager.	• “To Log Into the Web Manager” on page 128
3. You connect to the KVM port from the Connect to Server screen.	• “To Log Into a Server Connected to a KVM Port” on page 94 • “Connect to Server>Connect to KVM Ports” on page 144

Connecting to KVM Ports When Direct Access is Enabled

When direct access to KVM ports is enabled, a “port name” field appears on the Web Manager login screen, as shown in Figure 3-2.

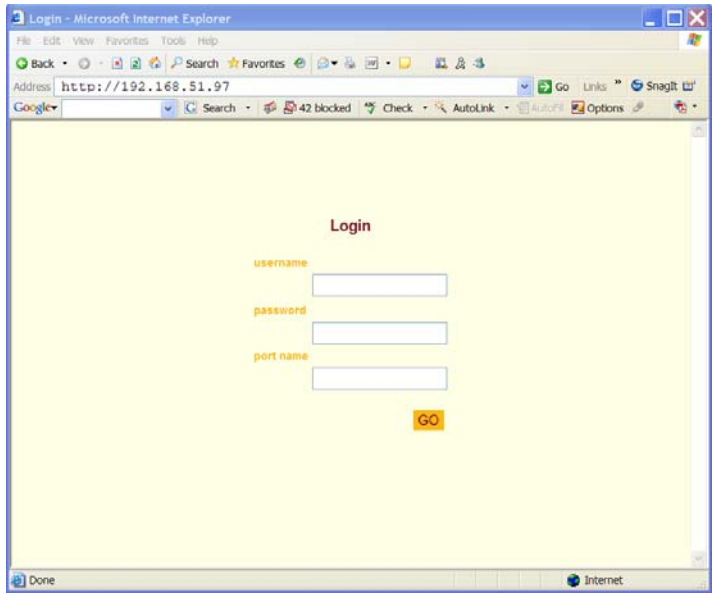


Figure 3-2: Web Manager Login Fields With KVM Port Direct Access Enabled, Only IP Address Entered

If you enter the port's alias or default portname along with the IP address you can connect directly to a KVM port without logging into the Web Manager first. The required format for specifying the port name along with the IP address is:

```
IP_address/login.asp?portname=port_alias
```

where *IP_address* is the IP address of the OnSite and *port_alias* is the default name or alias assigned to the KVM port.

After you enter the URL for the first time, you can save the URL as a bookmark or in your browser's favorites list and go directly to the port login later without typing in the entire URL. The "port" field is filled in with the port number when the Web Manager login window appears.

The example in the following figure shows `http://192.168.51.97/login.asp?portname=Port_1` entered in the Address field of a Microsoft Internet Explorer browser. The login screen displays empty "username" and "password" fields and a port field filled with the name of the port from the URL, in this case "Port_1."

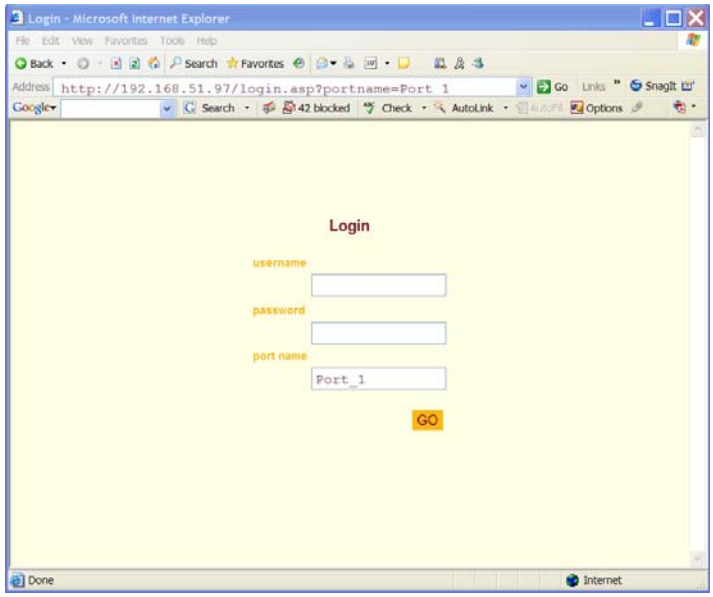


Figure 3-3: Web Manager Login Fields With KVM Port Direct Access Enabled and a Port Number in the URL

Table 3-2 gives the sequence for logging into servers connected to KVM ports *when direct access to KVM ports is enabled*.

Table 3-2: Connecting to KVM Ports Via Web Manager When Direct Access is Enabled

Login Sequence	Where Documented
1. You enter the OnSite's IP address in a browser. The Web Manager login screen comes up with "port name" field. 2. You enter your username and password. 3. You enter the KVM port name or port alias in the "port name field. OR 1. You enter the KVM port name in the URL along with the OnSite's IP address. The Web Manager login screen comes up with the "port name" field populated. 2. You enter your username and password. The AlterPath Viewer displays a login prompt.	• "To Connect to a KVM Port Through the Web Manager Login Screen" on page 133.

▼ *To Connect to a KVM Port Through the Web Manager Login Screen*

This procedure assumes that the OnSite administrator has enabled direct access to KVM ports. See "Direct Access to KVM Ports and KVM Port Authentication" on page 45 for more details, if needed.

1. Enter the IP address or DNS name of the OnSite alone or the IP address of the OnSite followed by the KVM port number (in the required format) in the address field of a browser.

   The format for entering the IP address and the KVM port number in the URL is:

```
IP_address/login.asp?portname=port_alias
```

where *IP_address* is the IP address of the OnSite and *port_alias* is the default port name or alias assigned to the KVM port.

- If DHCP is not enabled, use a static IP address assigned by the network administrator to the OnSite.
- If DHCP is enabled, enter the dynamically-assigned or fixed IP address.

The Web Manager login screen appears with the "port name" field. If you entered a KVM port alias in the URL, the "port name" field is filled in with the port alias you entered.

2. If you entered a KVM port alias in the URL, save the URL as a bookmark or in your favorites list in the browser.
3. Enter your account name in "username" field and the account's password in the "password" field.
4. If no port is listed in the "port" field, enter a port alias or number.
5. Click "Go."

   The AlterPath Viewer appears.

Serial Port Connection Options

Table 3-2 gives the sequence for logging into servers connected to serial ports *through the Web Manager.*

Table 3-3: Connecting to Serial Ports Via Web Manager

Login Sequence	Where Documented
1. You enter the OnSite's IP address or DNS name in a browser to bring up the Web Manager login screen, and you log into the Web Manager.	• "To Log Into the Web Manager" on page 128
3. You connect to the serial port from the Connect to Server screen.	• "To Log Into a Device's Console Through a Serial Port" on page 106 • "Connect to Server>Connect to Serial Ports" on page 144

Web Manager Inactivity Timeouts

An inactivity timeout period is set in the Web Manager for security. An administrator who knows the root password can change the timeout value as described in Chapter 8, “Miscellaneous Procedures.”

Web Manager Modes

The Web Manager has the two following modes when an administrative user is logged in:

- Wizard
- Expert

An administrative user can toggle between the modes by clicking one of the two buttons shown below.

- In Expert mode, the Wizard button appears.
- In Wizard mode, the Expert button appears.

The first time any administrative user logs in, the Wizard mode automatically comes up at the first step, to prompt the admin user to select a security profile before continuing.

At all other logins by administrative users, Expert is the default mode.

Common features of administrative user windows in both modes are described in:

Use of the Wizard mode is described in Chapter 5, “Web Manager Wizard Mode.”

Use of Expert mode is described in Chapter 6, “Web Manager for Administrators.”

▼ *To Switch Between Expert and Wizard Modes*

1. Log in as described in ““To Log Into the Web Manager” on page 128.
2. To change to another mode, select either the Wizard or Expert button.

Common Features of Administrative User's Windows

The features of all Web Manager windows for OnSite administrative users are described in the following sections.

Administrative User's Control Buttons

The following figure shows the control buttons that display at the bottom of the window when an administrative user is logged into the OnSite.

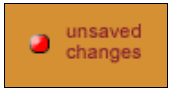
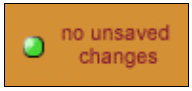
Figure 3-4: Web Manager Administrative Users' Buttons

The following table describes the uses for each control button. See Table 3-5 on page 137 for more details.

Table 3-4: Administrator's Control Buttons

Button Name	Use
back	Only appears in Wizard mode. Returns to the previous screen.
try changes	Save and apply changes. The changes are saved to the configuration files but not to the backup files, and the changes are preserved even when you reboot.
cancel changes	Overwrites the current state of the configuration files from the backup files.
apply changes	Save, apply, and back up changes.
reload page	Reloads the page.
Help	Brings up the online help.
next	Only appears in Wizard mode. Goes to the next step.

Table 3-4: Administrator's Control Buttons (Continued)

Button Name	Use
	The unsaved changes button appears on the lower right hand corner of the Web Manager and a red graphical LED blinks whenever the current user has made any changes and has not yet saved the changes.
	The no unsaved changes button appears and a green graphical LED appears when no changes have been made that need to be saved.

Trying, Saving, and Restoring Configuration Changes

The various options for trying, saving, and restoring configuration changes are summarized in the following table. Trying, saving, and restoring can be done in the OSD and on the Linux command line. The "Action" column shows the Web Manager actions.

Table 3-5: Options for Trying, Saving, and Restoring Configuration Changes

Option	Action	Result
Make changes	Enter information in any of the screens and click the OK or Done button	The "unsaved changes button" appears and a red graphical LED blinks. Changes are held in memory and not saved.
Try changes	Click the "try changes" button"	Updates (saves the changes in) the appropriate configuration files. Changes are preserved if you log in and log out again and even if you restart the system. The changes are not backed up unless "apply changes" is clicked. You can restore the backed-up configuration files by clicking "cancel changes."
Cancel changes	Click the "cancel changes" button	Restores the configuration files using the backup file that was created the last time changes were applied.

Table 3-5: Options for Trying, Saving, and Restoring Configuration Changes (Continued)

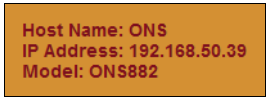
Option	Action	Result
Apply changes	Click the "apply changes" button	If "try changes" has not been previously clicked, updates the appropriate configuration files. The first time changes are "applied," creates a compressed copy of the configuration files in a backup directory. Subsequently overwrites the backed-up copy of the configuration files.

See "How Configuration Files Changes Are Managed" on page 574 for details about how to save, apply, and back up changes in the OSD and on the command line.

Logout Button, and OnSite Information

The following table describes the logout button and the other information that displays in the upper right corner of all Web Manager windows.

Table 3-6: Logout Button and Other Information in the Upper Right

WIndow Area	Purpose
	Click this button to log out.
	Displays the hostname and IP address assigned during initial configuration (see "Performing Basic Network Configuration" on page 67). Also displays the model name of the AlterPath OnSite.

▼ To Try or Save Web Manager Changes

Perform this procedure when a red graphical LED blinks in the "unsaved changes" button on the lower right hand corner of the Web Manager to indicate that changes have not been saved.

1. Click the "try changes" button to apply configuration changes, which can be restored by clicking the "cancel changes" button.
2. Click the "apply changes" button to save configuration changes.

Chapter 4
Web Manager for Regular Users

This chapter provides procedures and requirements for regular users to use the Web Manager to do the following tasks:

- Access computers and devices that are connected to ports on the OnSite
- Perform IPDU power management
- Change the current password
- Monitor the temperature of the OnSite

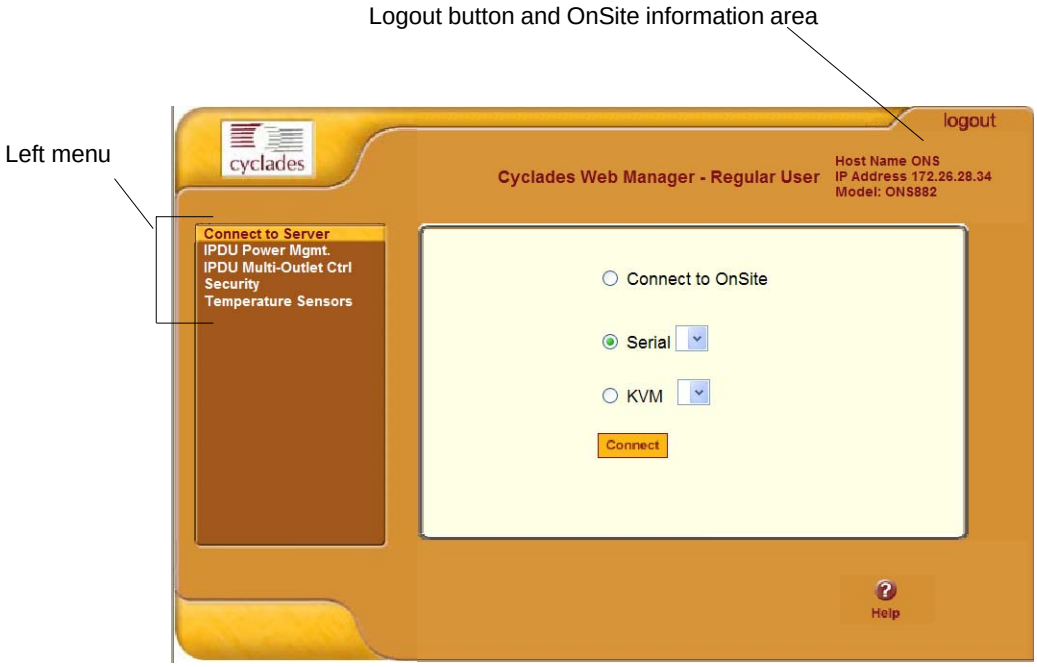
Regular users are users who have accounts configured on the OnSite and who are not in the "admin" group. (See "OnSite Port Permissions" on page 32, if needed, for details about the types of user accounts.)

For rules and prerequisites that must be in place before anyone can access the Web Manager, see Chapter 3, "Web Manager Introduction."

This chapter contains the following sections.

Features of Regular Users' Windows

The following figure shows features of the Web Manager when regular users log in.



The menu is on the left. The contents of the screen in the middle change according to which menu option is selected.

The following table describes the logout button, the information area, and the Help button.

Table 4-1: Logout Button and Other Information in the Upper Right

WIndow Area	Purpose
logout	Click this button to log out.
Host Name: ONS IP Address: 192.168.50.39 Model: ONS882	Displays the hostname and IP address assigned during initial configuration. Also displays the model name of the OnSite.

Table 4-1: Logout Button and Other Information in the Upper Right (Continued)

WIndow Area	Purpose
	Brings up the online help with information about the current screen.

The following table lists the sections where the options on the user's menu are described.

Connect to Server

On the "Connect to Server" screen, both regular users and administrative users can connect directly to the OnSite or connect to devices by connecting to the ports to which the devices are connected.

Authorization to access a port or perform power management is granted by the OnSite administrator when configuring a user account. A user who has permission to access ports or manage power is referred to as an authorized user.

Through this screen, authorized users can connect to the OnSite, to one of the serial ports, or to one of the KVM ports as described in the following sections.

- "Connect to Server>Connect to OnSite" on page 143
- "Connect to Server>Connect to Serial Ports" on page 144
- "Connect to Server>Connect to KVM Ports" on page 144

When a regular user or administrative user selects the "Connect to Server" option, the following screen appears.

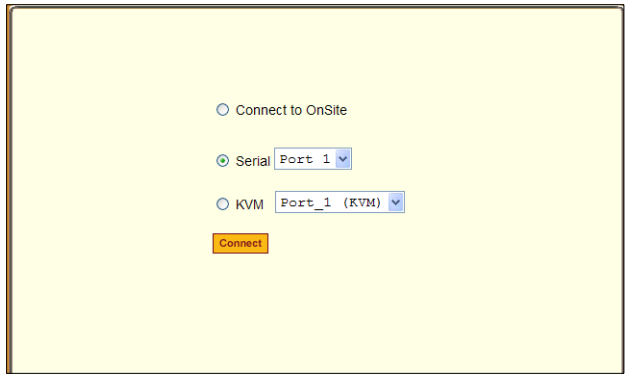


Figure 4-1: Connect to Server Screen [User]

On the latest versions of the OnSite hardware, an additional link appears at the lower right of the screen, as shown in the following screen example.

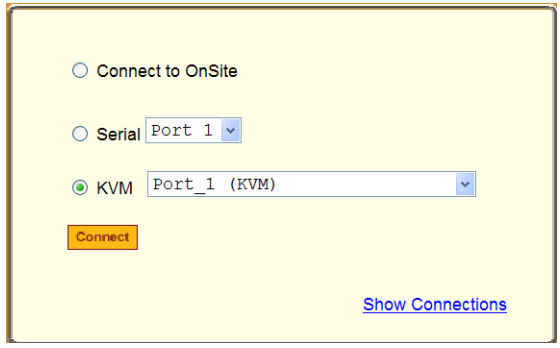


Figure 4-2: Connect to Server Screen With Show Connections Link

See “Connect to Server>Connect to KVM Ports” on page 144 for more details.

Connect to Server>Connect to OnSite

Clicking the “Connect to OnSite” radio button and clicking “Connect” brings up a Java applet running a secure SSH session and logs the user into the OnSite console, where the user has access to the OnSite’s command line.

An administrative user can use the `CLI` utility on the Linux command line. While connected to the OnSite console through the Web Manager, the administrative user cannot switch users to root. However, the administrative user can run commands as root by entering the `sudo` command followed by the command name.

The following figure shows the Java applet viewer running an SSH session. A “Connected to” message in a gray area at the top of the screen shows the IP address of the OnSite followed by the session type, “`ssh`.”

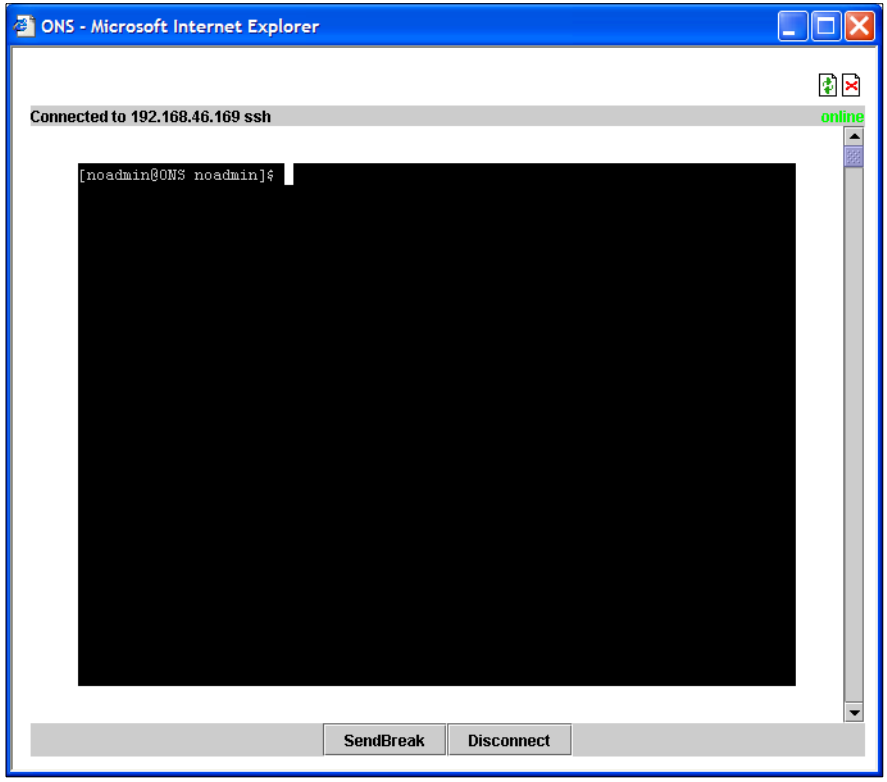


Figure 4-3: Java Applet Viewer Running an SSH Session on the OnSite

Connect to Server>Connect to Serial Ports

The list of serial ports displays the port names or administrator-defined aliases only for serial ports that the current user has permission to access. For administrative users all serial ports are listed.

Note: If you are a regular user and the list of serial ports is empty or does not include a port you need to access, contact the OnSite administrator for help.

Selecting a port number or alias and clicking “Connect” brings up a Java applet with a console connection to the device that is connected to the selected port. A “Connected to” message in a gray area at the top of the screen shows the IP address of the OnSite followed by the TCP port number.

Logins to connected devices may require authentication. Check with the OnSite administrator for the correct username and password to use. Login sessions are not ended when you terminate the connection, so you may be able to connect to a device and resume an existing session later, if the device has not logged you out because of the period of inactivity.

The Java applet display is similar to the one shown in Figure 4-3.

For the procedure, see “To Log Into a Device’s Console Through a Serial Port” on page 106.

Connect to Server>Connect to KVM Ports

A regular user’s authorization for KVM ports can be any of the following:

- No access
- Read only
- Read/Write
- Full access (Read/Write/Power management)

KVM Ports Menu

The “KVM” pull-down menu on the “Connect to Server” screen lists all the KVM port numbers or administrator-assigned aliases that the current user has permission to access. Administrative users see all KVM ports.

Note: If you are a regular user and the menu of KVM ports is empty or does not include a port you need to access, contact the OnSite administrator for help.

The following screen shows an example KVM port pull-down menu.

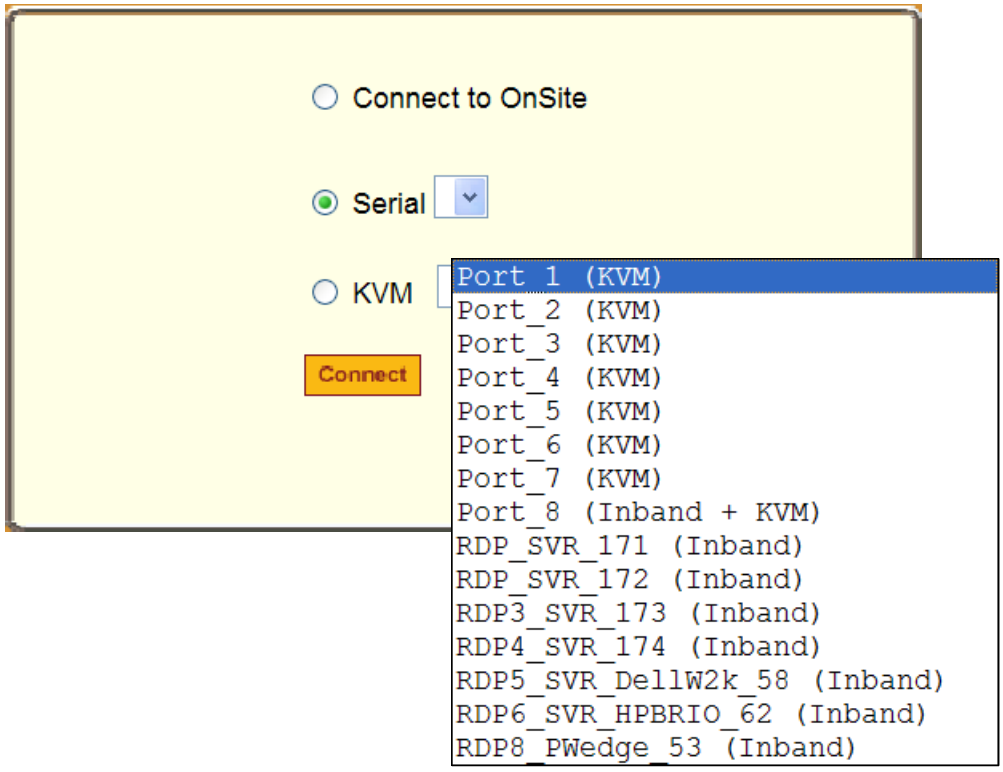


Figure 4-4: Example KVM Port Menu

After you select a port from the “KVM” menu, and click the “Connect” button, an AlterPath Viewer appears. See “Using the AlterPath Viewer” on page 77.

For the procedure, see “To Log Into a Server Connected to a KVM Port” on page 94.

Show Connections Link and Dialog

On the latest versions of the OnSite hardware, the “Show Connections” link appears at the lower right of the screen, as shown in the following screen example.

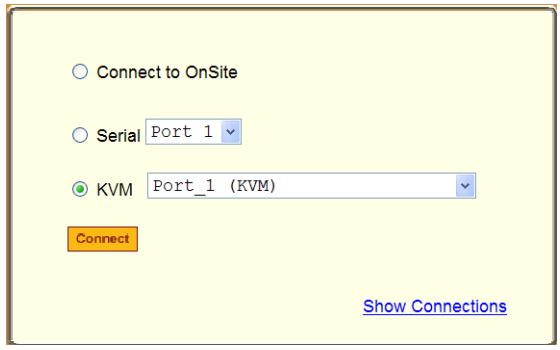


Figure 4-5: Connect to Server Screen With Show Connections Link

Clicking the “Show Connections” link while the KVM menu radio button is selected brings up a dialog. If no connection exists, a dialog like the following appears.

Figure 4-6: “Show Connections” Dialog With No Active Connection

If a connection exists, a dialog like the following appears.

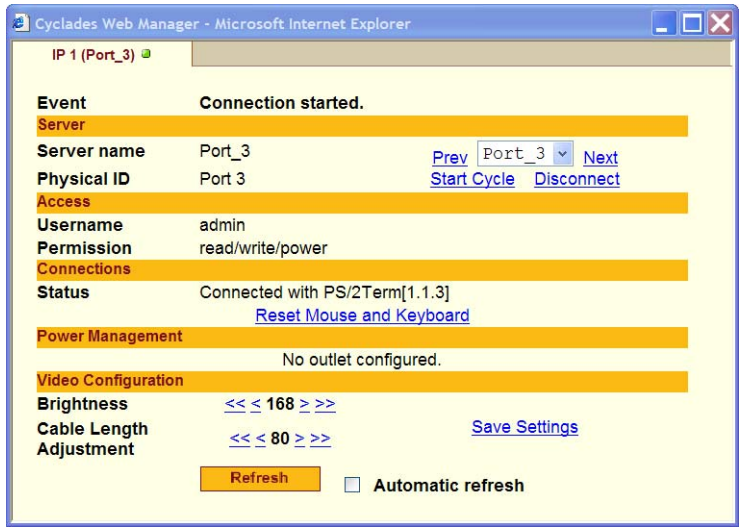


Figure 4-7: Show Connections Dialog

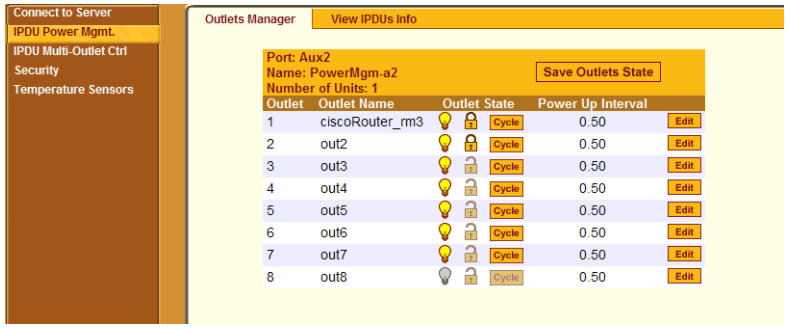
If the Show Connections Dialog is available with the OnSite version you are using, you can use the dialog to do the following:

- Go to the previous or next port on the list of ports you are authorized to access
- Start cycling through all the ports you are authorized to access
- View the status of the current connection
- Reset the mouse and keyboard
- Adjust the brightness
- Adjust for the length of cable between the OnSite and the server

On OnSite versions without the “Show Connection” capability, you can use other options described under “What You See When Connected to a KVM Port” on page 82 to do the same actions. For example, from the “Show Connections” dialog, you can make video adjustments. You can make the same adjustments by entering the hot key combination `Ctrl+k v` in the AlterPath Viewer while connected to bring up the Video Menu.

IPDU Power Mgmt. [User]

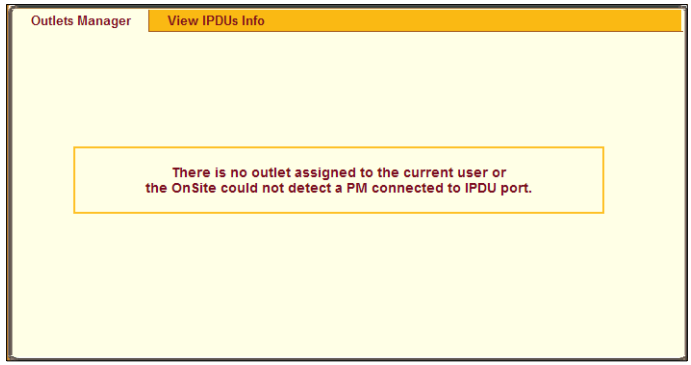
When you select the “IPDU Power Mgmt.” option in the Web Manager as a regular user, if you are authorized to manage outlets on an iAlterPath PM that is connected to one of the AUX ports, two tabs appear at the top of the screen, as shown in the following figure.



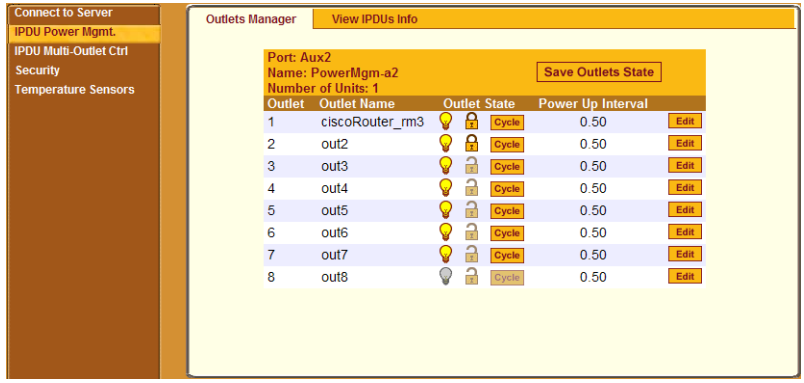
You can access screens from the tabs under IPDU Power Mgmt. to manage outlets, or to view IPDUs information:

IPDU Power Mgmt.>Outlets Manager [User]

When either an authorized users or an administrative user goes to IPDU Power Mgmt.>Outlets Manager, the message shown in the following figure appears either if the current user is a regular user who does not have permission to manage power on any outlets or if the OnSite cannot detect an AlterPath PM connected to an AUX port that has been configured for power management. Contact the OnSite administrator for help, if you see this message.



A screen like the one in the following figure appears if the current user is authorized to manage power on one or more outlets.



The screen shows separate entries for each port configured for power management. Each port's entry lists the number of IPDUs connected, and displays a line item for each outlet you are authorized to manage.

The authorized user can do the following for any listed outlet:

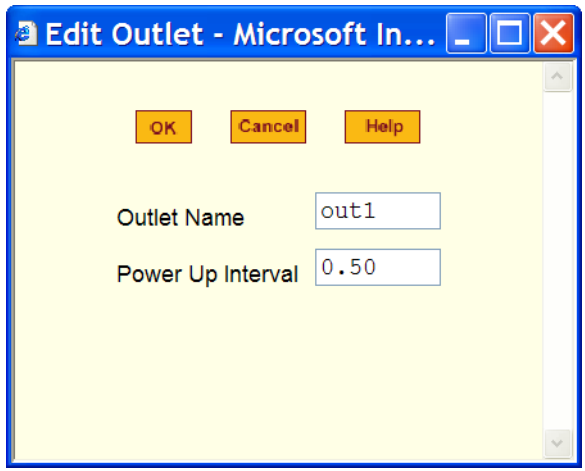
- Edit the power up interval.

  The power up interval is the number of seconds between when this currently-selected outlet turns on and the next outlet can be turned on.
- Cycle (turn power briefly off and then on again).
- Turn power off.
- Turn power on.

Yellow bulbs indicate an outlet is switched on. Gray indicates an outlet is switched off. An opened padlock indicates that an outlet is unlocked. A closed padlock indicates that an outlet is locked. An orange “Cycle” button is active next to each outlet that is on.

In the example below, outlet 1 is locked and outlet 2 is switched off and unlocked.

Clicking the Edit button brings up the dialog box shown in the following screen example, which allows you to specify a descriptive alias for the outlet and to change the power up interval. The power up interval is the amount of time (in seconds) that elapses after the selected outlet is turned on before another outlet can be turned on.



▼ *To View Status, Lock, Unlock, Rename, or Cycle Power Outlets*

1. Power Management IPDU>Outlets Manager.

   The “Outlets Manager” screen appears.

2. To power an outlet on or off, click the adjacent light bulb.
3. To lock or unlock an outlet, click the adjacent padlock.

4. To momentarily power an outlet off and then on again, click the adjacent “Cycle” button.
5. To change the outlet’s name or the power up interval, click the adjacent “Edit” button.

   The Edit Outlet dialog box appears.

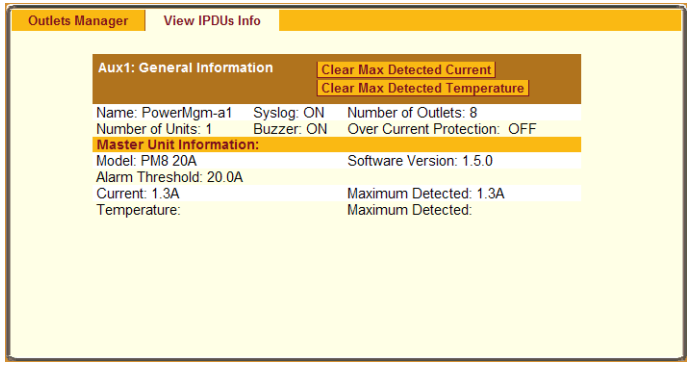
   a. To change the name assigned to the outlet, enter a new name in the “Outlet Name” field.
   b. To change the time between when this outlet is turned on and another can be turned on, enter a new number of seconds in the “Power Up Interval field.
6. Click OK.

   The Edit Outlet dialog box disappears and the Outlets Manager screen reappears.
7. Click the “Save Outlets State” button.
8. If you are an administrative user, click “apply changes.”

IPDU Power Mgmt.>View IPDUs Info

When an authorized user or an administrative user goes to IPDU Power Mgmt.>View IPDUs Info, a screen appears as shown in the following figure.

Note: Administrative users see three additional tabs, as shown in Figure 6-4.



A separate entry appears for each port that is configured for power management.

On the “View IPDUs Info” screen under IPDU Power Management, authorized users and administrative users can view the information shown in the following table about each port under “General Information.”

Table 4-2: General Port Information on the View IPDUs Info Screen

	Description	Example
Name	Either a default name or administrator-configured name.	PowerMgm-a1
Number of Units	The number of IPDUs connected to the port. The first IPDU is referred to as the master. Any other IPDUs daisy-chained off the first IPDU are referred to as slaves.	1
Number of Outlets	Total number of outlets on all connected IPDUs.	8
Buzzer	Whether a buzzer has been configured to sound when a specified alarm threshold is exceeded.	OFF
Syslog	Whether syslogging has been configured for messages from this IPDU.	ON
Over Current Protection	Whether over current protection is enabled (to prevent outlets from being turned on if the current on the IPDU exceeds the specified threshold).	OFF

You can view the following information about each IPDU (under Unit Information)

Table 4-3: IPDU Information on the View IPDUs Info Screen

	Description	Example
Model	AlterPath PM model number	PM8 20A
Software Version	PM firmware version	1.5.0
Alarm Threshold	Number of amperes that triggers an alarm or syslog message if it is reached	20.0A
Current	Current level on the IPDU	0.8A
Maximum Detected	Maximum current detected	1.3A
Temperature	Temperature on the AlterPath PM (only available on selected models that have temperature sensors)	
Maximum Detected	Maximum temperature detected	

You can also use the “Clear Max Detected Current” and “Clear Max Detected Temperature” buttons to clear those values.

▼ *To View and Reset IPDU Information [Expert]*

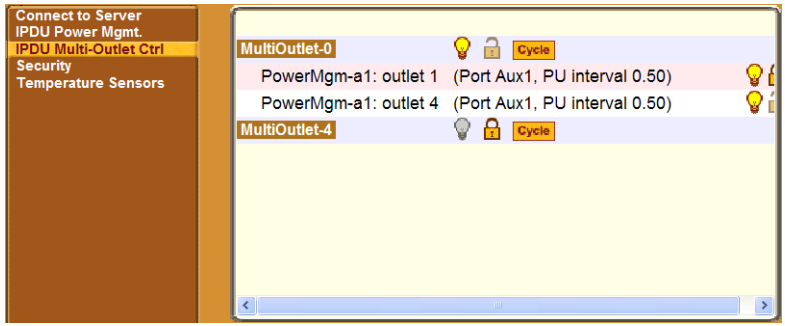
1. Power Management IPDU>View IPDUs Info

   The “View IPDUs Info” screen appears.

2. View the IPDU information as desired.
3. To clear the stored values for the maximum detected current, select the “Clear Max Detected Current” button.
4. To clear the stored values for the maximum detected temperature, click the “Clear Max Detected Temperature” button.

IPDU Power Mgmt.>IPDU Multi-Outlet Ctrl

When an authorized user selects the “IPDU Multi-Outlet Ctrl” menu option, a screen appears like the one shown in the following figure.



A multi-outlet device is a server or other device that has more than one power supply. On the “IPDU Multi-Outlet Ctrl.” screen, authorized users can view and manage the power on a group of outlets that provide power to a server or another device that has multiple power supplies, when the device is connected to a serial port and properly configured.

The outlets do not need to be on the same AlterPath PM IPDU.

Outlets on multiple IPDUs can be managed as a group from this screen.

See "Managing Multiple Outlets for how authorized users and administrators manage outlets for multi-outlet servers.

Managing Multiple Outlets

When an authorized user or administrative user selects the “IPDU Multi-Outlet Ctrl” option, the message shown in Figure 4-8 appears in the following cases:

1. No multi-outlet device is defined.
2. Power management for multiple outlets is not enabled for the serial port to which the device is connected.
3. No AUX port is connected to an AlterPath PM and configured for power management.

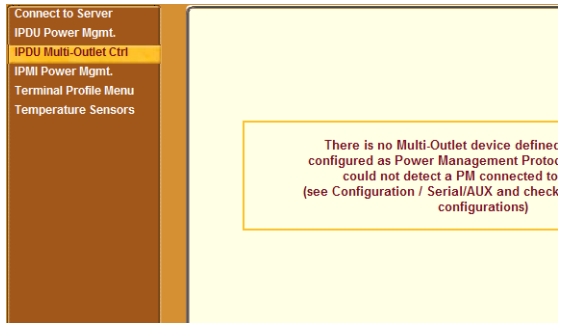


Figure 4-8: IPDU Multi-Outlet Ctrl Error Screen

A screen like the following appears when all the above-mentioned conditions have been met and the current user is authorized to manage power for a server that is connected to a serial port and that is plugged into multiple outlets.

Figure 4-9: IPDU Multi-Outlet Ctrl Screen

As shown in Figure 4-9, a separate entry appears for multi-outlet device, and each device is assigned a name according to the number of the serial port to which the device is connected. In this example, MultiOutlet-0 is the name assigned to the device connected to serial port 1 and MultiOutlet-4 is assigned to the device connected to serial port 5.

The light bulb, the lock icon, and the Cycle button on the line with the device name control the group of outlets for the device. The light bulb and lock icons next to the individual outlets display the status of each outlet, and they can be used to control the individual outlets.

The following table describes the icons in the first line of each group.

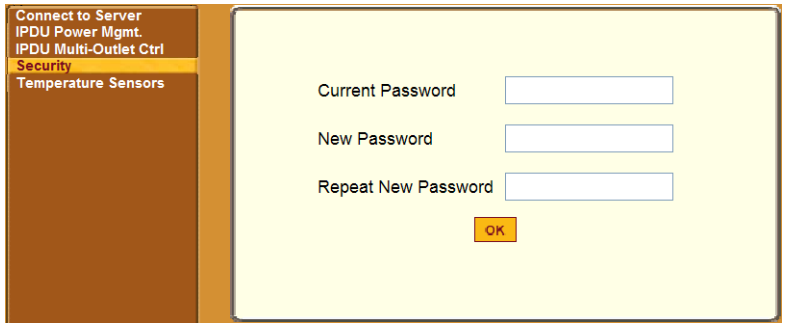
Table 4-4: IPDU Multi-Outlet Ctrl. Form Icons

Button	Purpose
	A grey light bulb indicates that the group is off. A yellow light bulb indicates that the group is on. Clicking the light bulb icon changes the power status of all of the outlets in the group.
	A grey and open lock indicates that the outlets are unlocked and can be powered on or off. A full-color and closed lock indicates that the outlet is locked and cannot be turned on or off. Clicking the lock changes the lock status of all of the icons in the group.
	Turn power briefly off and on again

Note: The “PU (Power Up) interval” parameter configured for each outlet affects the timing of the power up sequence. An outlet in a group turns on only after the power up interval specified for the previous outlet has elapsed. This PU interval can be configured through the “IPDU Power Mgmt.” screen. See “To View Status, Lock, Unlock, Rename, or Cycle Power Outlets” on page 150.

Security [User]

When you select the “Security” menu option as a regular user, a screen for changing your password appears as shown in the following figure.



▼ *To Change Your Password [User]*

1. Select the “Security” option from the left menu in the Web Manager Regular User screen.

   The “Security” screen appears.

2. Enter your current password in the “Current Password” field.
3. Enter the new password in the “New Password” and the “Repeat New Password” fields.
4. Click OK.

Temperature Sensors [User]

When you select the “Temperature Sensors” option as a regular user, the screen shown in the following figure appears.

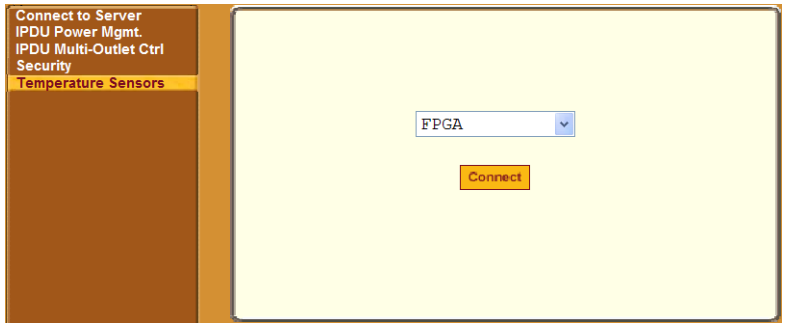


Figure 4-10: Web Manager Temperature Sensor Screen

The pull-down menu has an entry for each of the internal temperature sensors:

- FPGA (field programmable gate array)[
- Power supply
- CPU

Select one of the options to view a graph of readings from the selected temperature sensor, as shown in Figure 1-4 under “Monitoring Temperatures” on page 56.

See Table 1-27, “Temperature Graph Parameters,” on page 58 for descriptions of the defaults and allowed values you can specify to change the display.

▼ *To Monitor the OnSite’s Temperature*

Caution! The temperature should not exceed 115°F or fall below 50°F. If the temperature nears either of these values, take the appropriate action.

See “Monitoring Temperatures” on page 56 for background information, if needed, before performing this procedure.

1. Select the “Temperature Sensor” option from the left menu in the Web Manager.

   The “Temperature Sensor” screen appears.

2. Select “FPGA,” “Power Supply,” “CPU” from the pull-down menu.
3. Click “Connect.”

   The “Time X Temperature” dialog box appears.
4. Choose a display format.

   • To view the default format, do nothing.

   - OR -

   • Specify another display format.
5. Make any other desired changes.

   See Table 1-27, “Temperature Graph Parameters,” on page 58, if needed.
6. To apply any changes to the format, click “apply changes.”
7. To save any changes in a profile for later reuse, do the following.
   a. Click “Save Profile.”

      An “Enter Filename to Save Profile” dialog box appears.
   b. Enter a name for the profile and click OK.
   c. A “Profile saved” prompt appears.
   d. Click OK.
8. To apply a previously-defined profile, do the following.
   a. Select “Set Profile from File.”

      The “Select File to Set Profile From” dialog box appears.
   b. Select the desired profile’s file name.

      The temperature graph display changes to the format defined in the selected profile.
9. To clear the temperature display and start the plotting again at zero seconds, select “Clear Graph.”
10. To exit, click the X box at the upper right of the window.

Chapter 5
Web Manager Wizard Mode

This chapter describes the Web Manager Wizard mode on the OnSite.

The following table lists the topics in this chapter.

Wizard Screen Features

The following figure shows the features of the Wizard screens. Selecting an item from the left menu brings up a corresponding screen in the middle.

Figure 5-1: Example Web Manager Window in Wizard Mode

Selecting or deselecting some options displays additional fields. For example, if the DHCP checkbox is unchecked in the "Network Settings" step, fields for configuring the IP address and other network parameters appear.

The Wizard has six configuration steps listed in the left menu. As described under "Web Manager Modes" on page 135, the first time the admin user logs in after the OnSite is installed, the Wizard mode automatically presents the first step, because the admin user must select a security profile before continuing.

The buttons at the bottom of the screen are common to both Wizard and Expert mode, and they are described under "Common Features of Administrative User's Windows" on page 136.

Step 1: Security Profile [Wizard]

In Wizard Mode, when “Step 1: Security Profile” is selected, a screen appears like the one in the following figure.

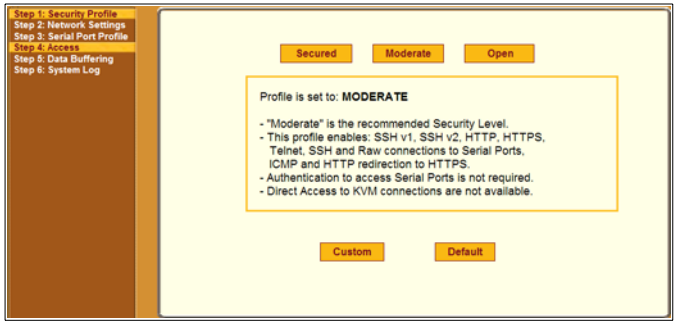


Figure 5-2: Web Manager Wizard Step 1: Security Profile

The screen identifies the name of the security profile currently in effect. An administrative user must do one of the following to configure a security profile that enforces the desired level of security for the OnSite:

- Select one of the preconfigured security profiles
- Configure a custom security profile and select it

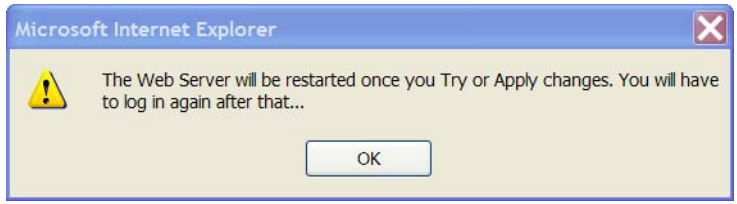
For more details about the services and features defined by preconfigured security profiles and what you can define in a custom profile, see “OnSite Security Profiles” on page 22.

As shown in Figure 5-2, the moderate security profile is selected by default. The features in the “Moderate” security profile are described in Table 1-10, “Moderate Security Profile Services/Features,” on page 24.

The screens for the three other security profiles are described in the following sections:

- “Step 1: Security Profile>Secured” on page 165
- “Step 1: Security Profile>Open” on page 166
- “Step 1: Security Profile>Custom” on page 167

When the administrative user clicks a button to select a security profile, a dialog appears like the one shown in the following screen example.



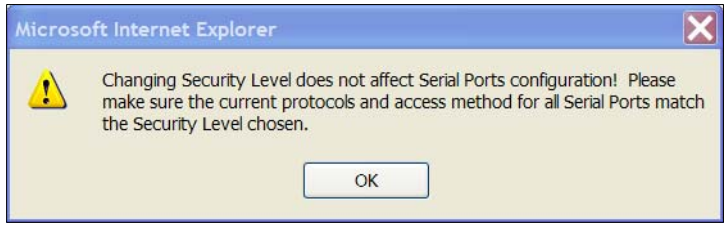
After the OK button is clicked, a screen reappears showing the newly-selected security profile's name.

When the administrative user creates a custom profile, the red "unsaved changes" button blinks. For example, the following figure shows the screen after the security profile is changed to "CUSTOMIZED," and the red "unsaved changes" light is lit.

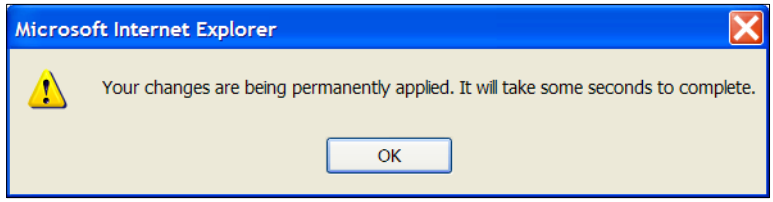
Figure 5-3: Customized Security Profile Screen

Whether or not the unsaved changes button lights, the administrative user must click the "apply changes" button to put the newly selected profile into effect. After the "apply changes" button is clicked, one of two dialogs appears next.

If the change has affected serial port access, a dialog appears like the one shown in the following screen example.



Otherwise, a dialog appears like the one shown in the following screen example.



The Web Manager restarts, and the administrative user must log in again.

Step 1: Security Profile>Secured

The following figure shows the screen for the “Secured” security profile.

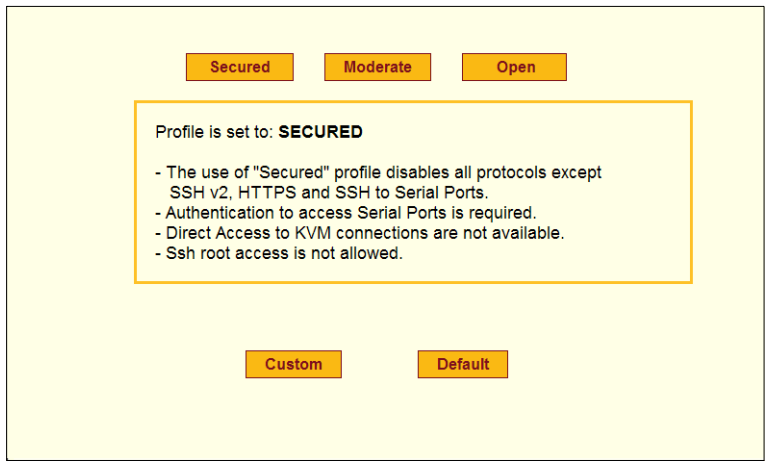


Figure 5-4: Secured Security Profile Screen

Note: If you select the “Secured” security profile, make sure to notify all users that they must use HTTPS when bringing up the Web Manager, because HTTP is disabled by the secured security profile. You must also make sure that X.509 certificates are included

The features in the “Secured” security profile are described in Table 1-12, “Secured Security Profile Services/Features,” on page 26.

Step 1: Security Profile>Open

The following figure shows the “Open” security profile screen.

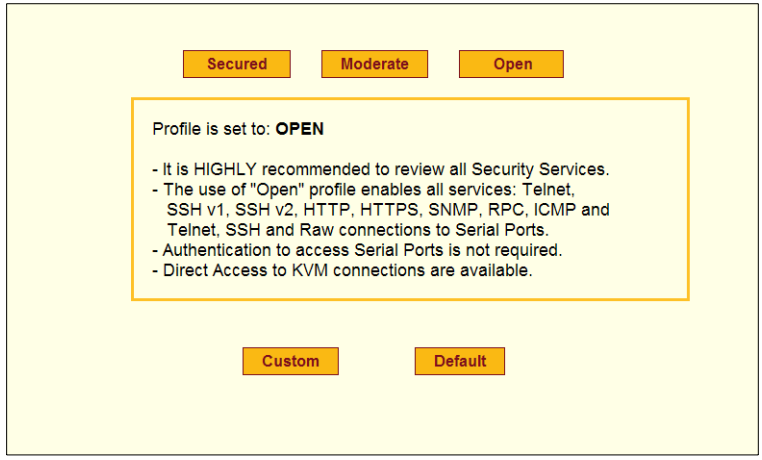


Figure 5-5: Open Security Profile Dialog

The features in the “Open” security profile are described in Table 1-11, “Open Security Profile Services/Features,” on page 25.

Step 1: Security Profile>Custom

The following figure shows the features that can be enabled and disabled in the dialog for the “Custom” security profile.

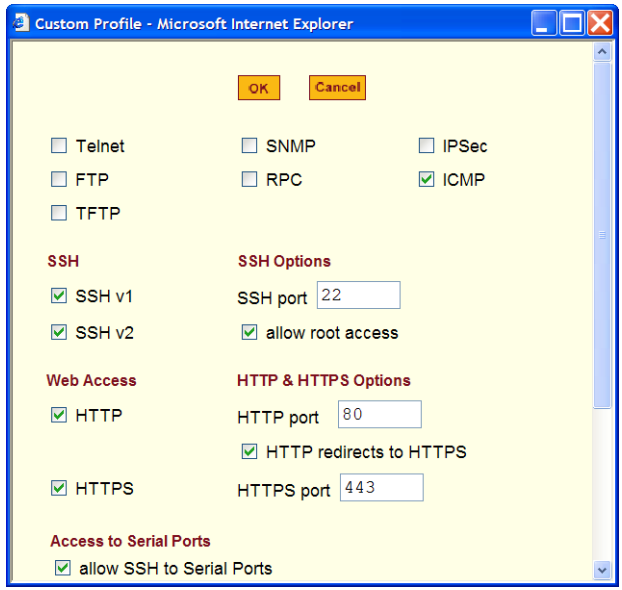


Figure 5-6: Custom Security Profile Dialog

The options that can be configured in a custom security profile are described in Table 1-9, “Services and Other Functions Defined in Security Profiles,” on page 23.

▼ *To Select or Configure a Security Profile—Wizard*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager for the Administrative User” on page 4, if needed.

   - If this is the first login by the admin user after OnSite installation, the Wizard mode appears by default. Go to Step 3.
   - If this is any subsequent login by an administrative user, go to Step 2.

2. Click the “Wizard” button.

3. Click the appropriate button to select a security profile.
4. If you select the “Custom” profile, a dialog appears with checkboxes next to all the configurable services and features.
5. If you are customizing a security profile, make sure the checkboxes are checked next to the services and features you want to be enabled and make sure the checkboxes are clear next to services and features you want to be disabled.
6. Click “OK.”

   The name of the security profile appears on the screen.

   - If you customized a security profile, the “unsaved changes” button blinks red. Go to Step 8.
   - If you selected any other security profile, a dialog appears. Go to Step 7.
7. Click “OK” on the dialog.
8. Click the “apply changes” button.

   A warning dialog appears. Go to Step 9.
9. Click “OK” on the dialog.

   The Web Manager restarts, and the login screen appears.
10. Log in if desired, to go to the next Wizard step.

Step 2: Network Settings [Wizard]

In Wizard Mode, selecting “Step 2: Network Settings” brings up a screen for reconfiguring existing network settings.

If the “DHCP” checkbox is not checked, the screen appears as shown in the following figure.

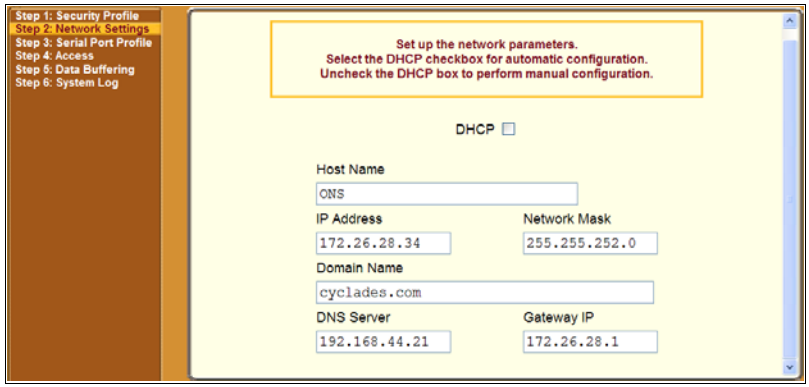


Figure 5-7: Web Manager Wizard Step 2: Network Settings screen—Without DHCP

If the “DHCP” checkbox is checked, the screen appears as shown in the following figure.

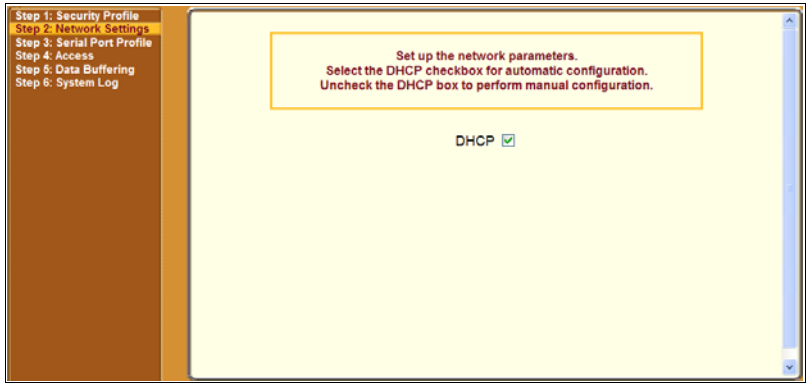


Figure 5-8: Web Manager Wizard Step 2: Network Settings Screen—DHCP

During initial setup of the OnSite, the administrator configures the basic network settings that are needed to enable logins through the Web Manager. (See “Performing Basic Network Configuration” on page 67, if desired, for more about the initial network configuration.) You can skip this step if the current settings are correct. Check with your network administrator if you are not sure.

Before making any changes to existing network settings, you may want to review “Collecting Basic Network Information” on page 57, which provides a form to record information you need to collect ahead of time. See “To Change Network Settings [Wizard]” on page 113 for the procedure.

In Expert mode, under Configuration>Network, you can specify additional networking-related information and perform other advanced configuration tasks. See “Network” on page 219.

▼ *To Configure Network Settings [Wizard]*

1. Collect any IP addresses or other network information to change.

   See the list of network information to collect under “Collecting Basic Network Information” on page 2, if needed.

2. In Wizard mode, go to “Step 2: Network Settings.”

   If the “DHCP” checkbox is checked, only the checkbox appears below the instructions.

Note: If DHCP is enabled, a local DHCP server assigns the OnSite a dynamic IP address that can change. The administrator chooses whether or not to use DHCP during initial setup. The initial setting may have been changed since initial configuration.

---

3. If the “DHCP” checkbox is not checked, enter the network information in the fields.
4. Click the “apply changes” button.
5. If appropriate, press the Next button or select “Step 2: Access” from the left menu**.**

Step 3: Serial Port Profile [Wizard]

In Wizard mode, selecting “Step 3: Serial Port Profile” brings up a screen for changing parameters that apply to all serial ports on the OnSite.

Note: The values specified here must match the values on all devices connected to the serial ports. The defaults are correct for most devices. Use this screen only if you need to change the parameters.

The screen appears as shown in the following figure with the default options.

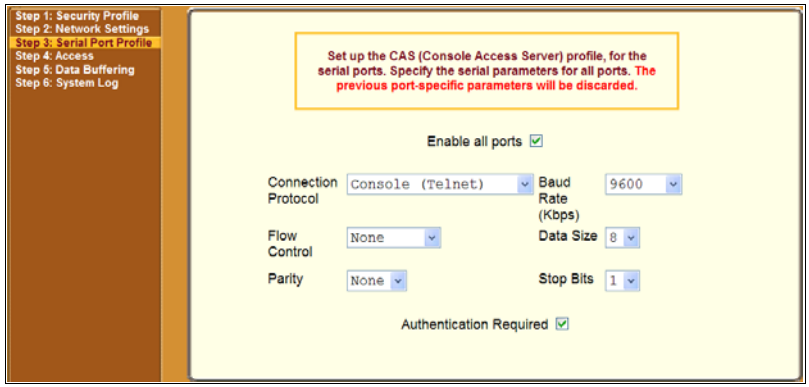


Figure 5-9: Web Manager Wizard Step 3: Serial Port Profile Screen

The following table lists the parameters and the options for each parameter, and it provides additional related information.

Table 5-1: Serial Port Profile Parameters and Usage

Parameter	Options	Description
Connection Protocol	Console (Telnet) [Default] Console (SSH) Console (TelnetSSH) Console (Raw)	Sets the method that must be used to connect to devices that are connected to serial ports. Console (SSH) is recommended because it encrypts data and authentication information. Console (TelnetSSH) allows users to connect using either protocol. Console (Raw) is for unnegotiated plain socket connections.

Table 5-1: Serial Port Profile Parameters and Usage (Continued)

Parameter	Options	Description
Flow Control	None [Default] Hardware Software	Must match the flow control method of the devices connected to all serial ports.
Parity	None [Default] Odd Even	Must match the parity used by the devices connected to all serial ports.
Baud Rate (Kbps)	9600 [Default] Options range from 2400–921600 Kbps	Must match the baud rates of the devices connected to all serial ports.
Data Size	8 [Default] Options range from 5–8	Must match the number of data bits used by the devices connected to all ports.
Stop Bits	1 [Default] Options are either 1 or 2	Must match the number of stop bits used by the devices connected to all ports.
Authentication Required	Check for Yes. Leave Unchecked for No [Default]	If the radio button is checked, user authentication is enforced using the local `passwd` database. To specify other authentication methods such as LDAP, RADIUS, TACACS+, or Kerberos, go to Expert mode and select Configuration>Authentication. For the procedure, see “To Configure Serial Port Access for Users [Expert]” on page 240.

Expert mode provides many additional options for custom configuration of serial ports. To assign an alias to a serial port or to specify other differing values for individual serial ports or groups of serial ports, see “Configuration>Serial/AUX” on page 227. Use Expert mode, for example, if you want to specify any of several other connection protocols, including, for example, PPP and SLIP.

Note: You cannot configure KVM ports in Wizard mode. To configure KVM ports, see “Configuration>KVM” on page 212.

The following table lists the tasks for configuring serial ports with links to where they are documented.

Table 5-2: Tasks for Configuring Serial Ports

Table 5-2: Tasks for Configuring Serial Ports

To Configure a Trigger for SNMP Trap Notification for Serial Ports Expert]	Page 272

▼ To Configure Serial Ports [Wizard]

Perform this procedure only if the serial ports are connected to the console ports on devices. If the serial ports are connected to dumb terminals, you can configure them only in Expert mode. Perform this procedure only if the following are both true:

- The serial ports are connected to console ports on devices.
- All the connected devices run at the same speed and with the same values.
- The values you specify here are the same as those in effect on the connected devices.

For details about the applicable values, see Table 3-5, “Serial Port Profile Parameters and Usage,” on page 115.

If all the connected devices do not run at the same speed and with the same values, configure individual settings in Expert mode as described under “Serial” on page 192.

1. In Wizard mode, go to “Step 3: Port Profile.”
2. To change the connection protocol, select “Console (Telnet),” “Console (SSH),” “Console (TelnetSSH), or “Console (Raw)” from the “Connection Protocol” pull-down menu.

   The default is “Console (Telnet).”
3. To change the flow control, select “None,” “Hardware,” or “Software” from the “Flow Control” pull-down menu.

   The default is None.
4. To change the parity, select “None,” “Odd” or “Even” from the “Parity” pull-down menu.

   The default is “None.”
5. To change the baud rate, select an option from 2400 to 921600 Kbps from the “Baud Rate” pull-down menu.

   The default is 9600, which is the most common baud rate for devices.

6. To change the data size, select an option from 5 to 8 from the “Data Size” pull-down menu.

   The default is 8.

7. To change the stop bits, select 1 or 2 from the “Stop Bits” pull-down menu.

   The default is 1.

8. To change whether authentication is required, check the “Authentication Required” checkbox for Yes or leave it unchecked for No.

9. Click the “apply changes” button.

10. If desired, go to ““To Add a User [Wizard]” on page 177.

Step 4: Access [Wizard]

In Wizard mode, selecting “Step 4: Access” brings up a screen for adding or deleting users and for setting or changing passwords. The screen appears as shown in the following figure.

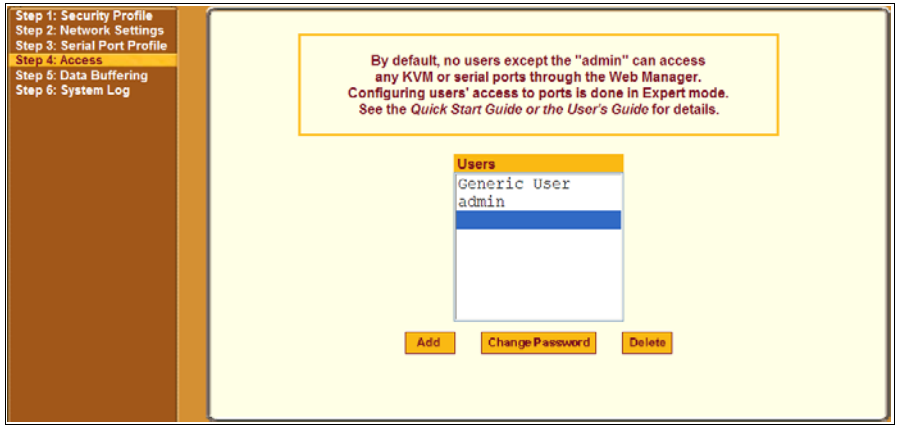


Figure 5-10: Web Manager Wizard “Step 4: Access” Screen

Use this screen if you want to add or delete user accounts.

The Access screen lists the currently defined Users and has three buttons: “Add,” “Change Password,” and “Delete.”

In the Users list, by default, are two user accounts that cannot be deleted:

- Admin
- Generic User

The Admin (the “admin” account) has access to all functions of the Web Manager and has access to all ports on the OnSite.

The Generic User defines the KVM port access permissions for all users except the admin and root users. Any new regular user account automatically inherits the KVM port access permissions configured for the Generic User.

For more background about the hierarchy of KVM port permissions, see “Understanding KVM Port Permissions” on page 32 and “KVM Port Permissions Hierarchy” on page 34.

If you click the “Add” button, the following screen appears.

The following table defines the information required in the fields.

Table 5-3: Add User Dialog: Field Names and Definitions

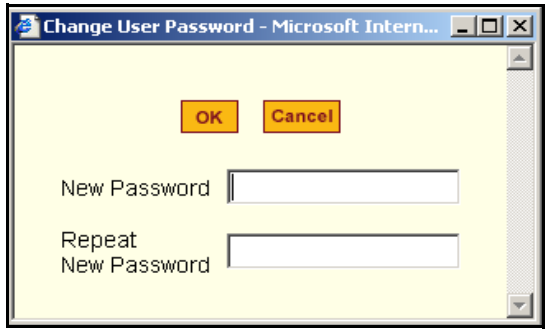
Field Name	Definition
User Name	The username for the account being added.
Password	The password for the account.

Table 5-3: Add User Dialog: Field Names and Definitions (Continued)

Field Name	Definition
Group	The choices in the "Group" menu are "Regular User" [Default] or "Admin." **Note:** To configure a user to be able to perform all OnSite administration functions, select the "Admin" group. See "Types of Users" on page 18, if needed, for more background.
Shell	Optional. The default shell when the user makes a `ssh` or `telnet` connection with the switch. Choices are: `sh` [Default] or `bash`.
Comments	Optional notes about the user's role or configuration.

Note: To perform advanced configuration for users and groups, such as, for example, to restrict user access to KVM ports, or to create a group, go to Expert>Configuration >Users and Groups.

If you click the "Change Password" button, the following screen displays.



▼ *To Add a User [Wizard]*

1. In Wizard mode, go to Step 4: Access.

   The Access screen displays.

2. Click Add.

   The "Add User" dialog box appears.

3. Enter the username and password in the “User Name” and “Password” fields, and enter the password again in the “Repeat Password” field.
4. Select from the “Group” menu options.
   a. To create a regular user account without administrator privileges, select “Regular User” [Default] from the “Group” pull-down menu on the left.
   b. To create an account with administrator privileges, select “Admin” from the “Group” pull-down menu on the left.
5. Optional: Enter the default shell in the “Shell” field.
6. Optional: Enter comments to identify the user’s role or configuration in the “Comments” field.
7. Click OK.
8. Click the “apply changes” button.

▼ *To Delete a User [Wizard]*

1. In Wizard mode, go to “Step 4: Access.”

   The “Access” screen displays.

1. Select the user name to delete.
2. Click “Delete.”
3. Click “apply changes.”

▼ *To Change a Password [Wizard]*

Note: Leaving the default admin password unchanged leaves the OnSite and connected devices open to anyone who knows the default password and the OnSite’s IP address. For security’s sake, make sure the admin password has been changed from the default “cyclades.”

---

1. In Wizard mode, go to “Step 4: Access.”

   The “Access” screen displays.

2. Select the name of the user whose password you want to change.

For example, select “admin.”

3. Click “Change Password.”

   The “Change User Password” dialog box displays.

4. Enter the new password in both fields, and then click OK.
5. Click “apply changes.”

Step 5: Data Buffering [Wizard]

In Wizard mode, selecting “Step 5: Data Buffering” brings up a screen for setting up the storage of console data to a data buffer file. The values set here apply to all serial ports. Data buffering allows a site to save a record of all communications during a serial port connection session. You can set up data buffer files to be stored either in local files on the OnSite’s Flash memory or on the hard disk of an external server, such as a syslog server.

The screen displays different fields depending on whether “Local” or “Remote” is selected from the “Enable Data Buffering” pull-down menu. The following figure shows the screen when Local is selected.

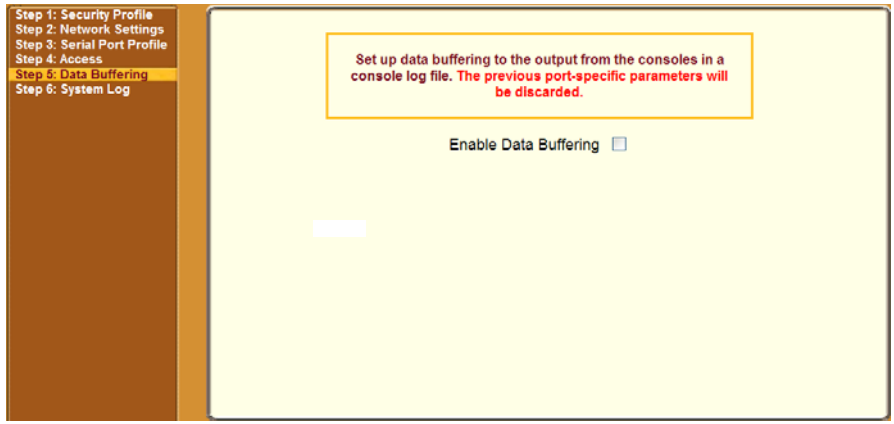


Figure 5-11: Wizard “Step 5: Data Buffering” Screen—Local

The following figure shows the screen when Remote is selected.

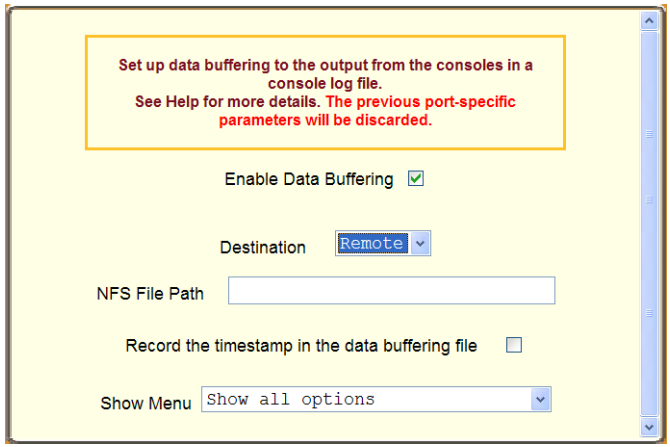


Figure 5-12: "Step 5: Data Buffering" Screen—Remote

Make sure that enough disk space is available to store the files in the location you select. Sequentially-written files can quickly grow to exceed the storage capacity of the local flash memory or remote hard drive. Data buffering should only be done if processes are in place to monitor the stored data. The following table shows the differences between remote and local data buffering.

Table 5-4: Differences Between Remote and Local Buffering

Option	Description
Remote server	Data is stored linearly in files. The NFS server must already be configured with the mount point shared (exported). In linear mode, data is written into a continuous sequence of files, and the file spaces is not reused. The administrator needs to allow enough space for the expected amount of data and take measures, such as moving unneeded data files off line, to ensure that the data does not outgrow the available space.

Table 5-4: Differences Between Remote and Local Buffering (Continued)

Option	Description
Local files	Set a file size greater than zero. Make sure the file size does not exceed the space available on the OnSite's flash memory. If needed, you can supplement the flash memory module by installing a flash memory card (with an adapter) or other storage device in a PCMCIA slot; see "PCMCIA Card Slots" on page 13 for the supported PCMCIA cards. Local data buffering stores data in *circular* or *linear* mode. In circular mode, data is written into the specified local data file until the upper limit on the file size is reached; then the data is overwritten starting from the top of the file as additional data comes in. Circular buffering requires the administrator to set up processes to scrutinize the data during the time window before the data is overwritten by new data.

You can perform advanced configuration in Expert mode including the option of setting up data buffering differently for individual ports or groups of ports.

▼ *To Configure Data Buffering [Wizard]*

1. In Wizard mode, go to "Step 5: Data Buffering."
2. Click the "Enable Data Buffering" checkbox.

   The "Destination" pull-down menu appears.
3. Select the location for the data files from the "Destination" pull-down menu (either "Local" or "Remote").

   Additional pull-down menus and fields appear, depending on which destination is selected.
4. When the destination is local, perform the following steps.
   a. From the "Mode" pull-down menu, select "Circular" or "Linear" data buffering.
   b. Type a file size in bytes into the "File Size (Bytes)" field.

      The file size cannot be zero.
5. When the destination is remote, perform the following steps.

a. In the “NFS File Path” field, enter the pathname for the mount point of the directory where data buffer file is to be stored.

For example, if the mount point directory’s pathname is `/var/adm/ONSmessages`, enter `/var/adm/ONSmessages` in the field.

Note: The NFS server must already be configured with the mount point shared (exported), and the shared directory from the NFS server must be mounted on the OnSite.

---

b. To cause a timestamp to be saved with the data in the data buffer file, check the “Record the timestamp in the data buffering file” checkbox.

c. Select an option from the “Show Menu” pull-down menu.

The choices are: “show all options,” “No,” “Show data buffering file only,” and “Show without the erase options.”

6. Click “apply changes.”

Step 6: System Log [Wizard]

In Wizard mode, selecting “Step 6: System Log” brings up a screen for identifying one or more syslog servers to receive syslog messages from the OnSite and for IPDUs, if IPDU syslogging is configured. The screen appears as shown in the following figure.

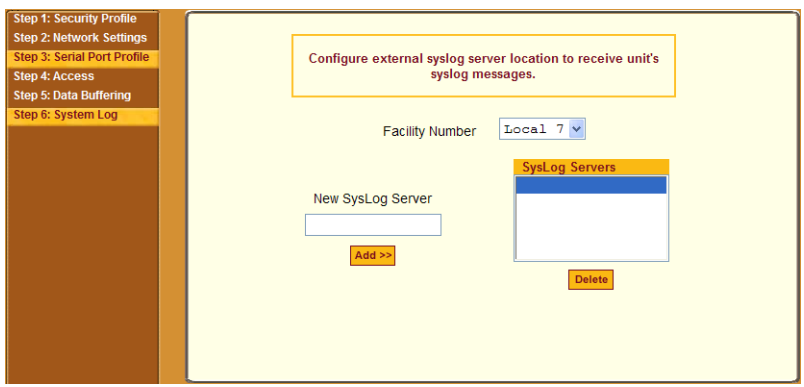


Figure 5-13: Wizard “Step 6: System Log” Screen

Before setting up syslogging, make sure an already-configured syslog server is available on the same network as the OnSite. Obtain the following information from the syslog server's administrator.

- The IP address of the syslog server
- The facility number for messages coming from the OnSite

  See "Notifications, Alarms, and Data Buffering" on page 40, if needed, for more background on logging and on how facility numbers are used.

You can configure syslog servers for messages relating to serial or KVM ports, to OnSite traffic, and to IPDU events of interest in Expert mode. The following table has links to the wizard procedures for adding and deleting a syslog server and for other related procedures.

▼ *To Add a Syslog Server [Wizard]*

This procedure assumes you have the following information:

- The IP address of the syslog server
- The facility number for messages coming from the OnSite

1. In Wizard mode, go to "Step 6: System Log."

   The System Log screen displays.

2. From the Facility Number drop-down menu, select the facility number.
3. In the New Syslog Server field, enter the IP address of a syslog server, and then select the Add button. (Repeat this step until all syslog servers are listed.)
4. The new server(s) appear in the Syslog Servers list.
5. Click "apply changes."

▼ *To Delete a Syslog Server [Wizard]*

1. In Wizard mode, go to “Step 6: System Log.”

   The System Log screen displays.

2. From the Syslog Server list, select the syslog server that you want to delete from the current facility location, and then select Delete.

3. Click “apply changes.

Chapter 6
Web Manager for Administrators

This chapter is for administrative users who use the Web Manager to configure the OnSite and who can also use the Web Manager to access connected devices. Two types of administrative users can access all the Web Manager configuration and access functions described in this chapter:

- A user who knows the password for the “admin” account, which is configured by default
- An optionally-added administrative user, who is a regular user whose account is in the “admin” group

  See “Users & Groups” on page 168 for how the admin adds an account configured for OnSite administration, if needed. For more background about the differences between user types, see “Types of Users” on page 18, if needed.

Before following the procedures in this chapter, review “Prerequisites for Using the Web Manager” on page 16, if needed, to make sure that the administrative user can connect to the Web Manager. Also see “To Log Into the Web Manager” on page 128 and “To Connect to a KVM Port Through the Web Manager Login Screen” on page 133, if needed.

The sections listed in the following table provide background information related to OnSite administrators’ use of the Web Manager, including explanations of the types of information to be entered in the screens and links to procedures.

Common Tasks

Common OnSite administration tasks are listed in the following table.

Table 6-1: Common OnSite Administration Tasks (Sheet 1 of 3)

Task	Where Documented
At first login, do the following: • Select a security profile • Configure basic networking • Configure serial port access • Add user accounts • Change the admin password • Configure data buffering • Configure syslogging **Note:** These wizard steps can be accessed again at any time. All Wizard steps can be achieved in Expert mode.	• "To Configure Network Settings [Wizard]" on page 170 • "To Configure Serial Ports [Wizard]" on page 174 • "To Add a User [Wizard]" on page 177 • "To Change a Password [Wizard]" on page 178 • "To Configure Data Buffering [Wizard]" on page 181 • "To Add a Syslog Server [Wizard]" on page 183
• Set up other users to access connected devices without those users being able to make changes to the OnSite configuration. • Set up other users to share all administration of the OnSite.	• "To Add a User [Expert]" on page 294
Authorize users or groups to access specific ports. (By default, regular users do not have access to KVM or serial ports.)	• "To Assign KVM Ports to a User or Group [Expert]" on page 296 • "To Configure Serial Port Access for Users [Expert]" on page 240
Authorize users to manage outlets on connected AlterPath PMs.	"To Configure Users to Manage Power Outlets on IPDUs [Expert]" on page 196
Enable direct login to KVM ports by authorized users from the Web Manager login screen.	"To Enable Direct Access to KVM Ports [Expert]" on page 214

Table 6-1: Common OnSite Administration Tasks (Sheet 2 of 3)

Task	Where Documented
Configure local or remote data buffering (to save console input to a log file) and specify alarms for trigger events on serial port(s).	• ““To Configure Data Buffering for Serial Ports [Expert]” on page 243 • “To Choose a Method for Sending Notifications for Serial Port Data Buffering Events [Expert]” on page 270
Configure logging of system messages to a syslog server.	• “To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]” on page 198 • “To Configure Syslogging and Message Filtering [Expert]” on page 304
Configure power management for one or both of the AUX ports (if the port is connected to an optional AlterPath PM or other supported IPDU device).	• “To Configure an AUX Port for IPDU Power Management [Expert]” on page 266 Also see the procedures under “Access>IPDU Power Mgmt.” on page 193 including: • “To View Status, Lock, Unlock, Rename, or Cycle Power Outlets” on page 150 • “To View and Reset IPDU Information [Expert]” on page 153
Configure servers for IPMI power management.	“Access>IPMI Power Mgmt.” on page 204
Choose among authentication methods and specify authentication servers for the following:	
• Logins to the OnSite	• “To Configure an OnSite Login Authentication Method [Expert]” on page 277
• Logins to devices through KVM ports.	• “To Configure an Authentication Method for Direct Access to KVM Ports [Expert]” on page 217

Table 6-1: Common OnSite Administration Tasks (Sheet 3 of 3)

Task	Where Documented
• Logins to devices through serial ports.	• "To Configure a Serial Port Authentication Method [Expert]" on page 241
Specify encryption levels for communications between the OnSite and user computers connected to KVM ports.	"To Configure IP Users (KVM Over IP) Sessions [Expert]" on page 222
Configure rules for the OnSite to filter packets like a firewall.	• "Configuration>Network>Firewall Configuration" on page 327 • "To Add a Chain [Expert]" on page 339 • "To Edit a Chain [Expert]" on page 340 • "To Edit a Rule [Expert]" on page 341 • "To Add a Rule [Expert]" on page 341

Expert Mode

If you are in Wizard mode and need to perform advanced configuration, click the Expert button at the bottom of the left menu to switch to Expert mode. The Wizard button displays at the lower left when you are in Expert mode.

The following figure shows a typical Web Manager window when the administrative user is logged in and is in Expert mode.

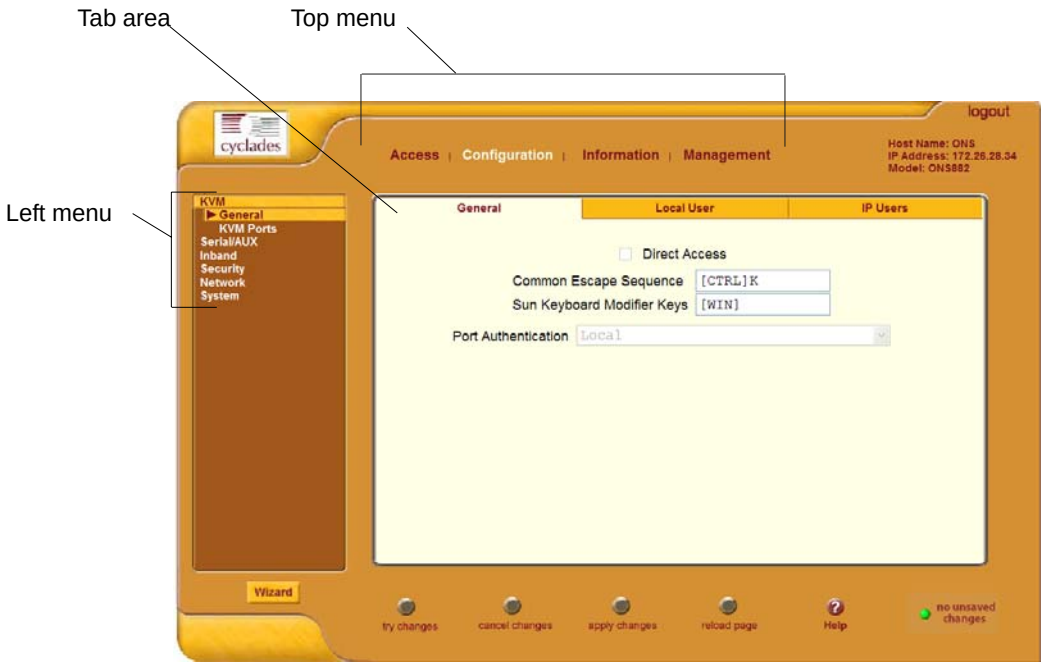


Figure 6-1: Web Manager Example Screen

Selecting an item from the top menu changes the list of menu options displayed in the left menu.

An option in the left menu (such as “KVM” in the preceding figure) may have several related screens associated with it. Selecting a tab labeled with the name of the related screen or selecting the screen’s name in the left menu brings up the related screen.

Note: Shortcuts are often used to indicate how to get to Web Manager screens. For example, a step telling the user to access the “IP Users” screen in the right tab in the previous figure would use this convention, “Go to Configuration>KVM>General >IP Users in Expert mode.”

Overview of Menus and Screens in Expert Mode

The following figure shows all screens in Expert mode.

Access

Under “Access” in Expert mode, six options appear in the left menu, as shown in the following figure.

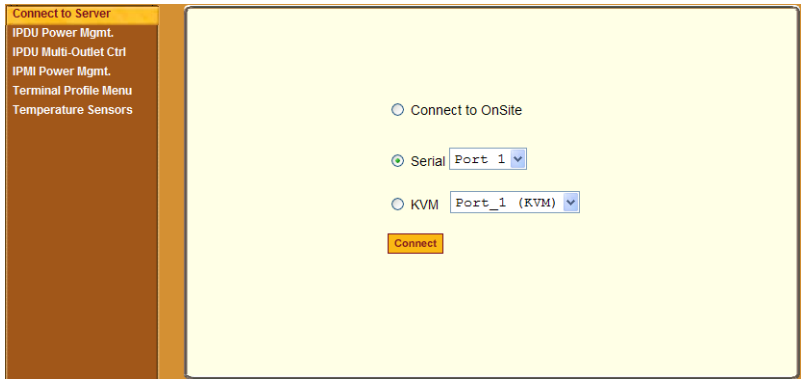


Figure 6-2: Web Manager Access Menu Options

The options in the Connect to Server screen are the same both for regular users and administrative users, as described under “Connect to Server” on page 141.

The remaining options listed below are different for administrative users than they are for authorized users.

Access>IPDU Power Mgmt.	Page 193
Access>IPDU Multi-Outlet Ctrl	Page 201
Access>IPMI Power Mgmt.	Page 204
Access>Terminal Profile Menu	Page 201
Access>Temperature Sensors	Page 210

The following table lists the related procedures and where they are documented.

To Connect to the OnSite Console as admin [Expert]	Page 193
To Log Into a Device’s Console Through a Serial Port	Page 106
To Log Into a Server Connected to a KVM Port	Page 94

▼ *To Connect to the OnSite Console as admin [Expert]*

This procedure logs the administrative user into the OnSite console as "admin" in a `ssh` session.

1. While logged into the OnSite as an administrative user, go to Access>Connect to Server.
2. Click the "Connect to OnSite" radio button.
3. Click the "Connect" button.

   A Java applet viewer appears with an admin prompt.

Access>IPDU Power Mgmt.

On the "IPDU Power Mgmt" screens under "Access" in Expert mode, an administrative user can manage power for devices that are plugged into outlets on an AlterPath PM IPDU.

Selecting the "IPDU Mgmt." option under "Access" in Expert mode brings up the five tabs shown in the following figure.

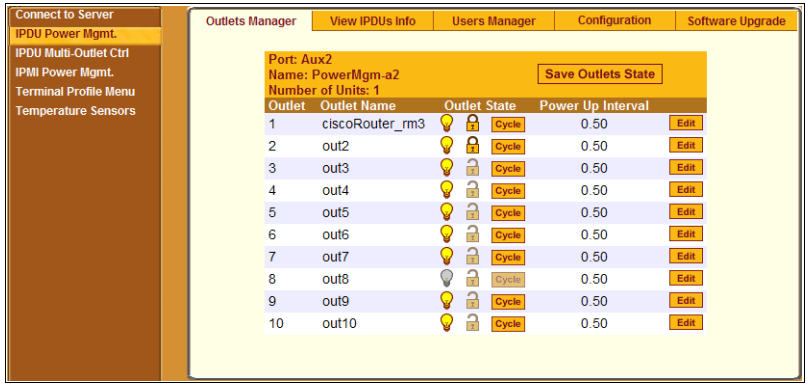


Figure 6-3: Web Manager IPDU Power Mgmt. Tab Options

Users can manage power using the tabbed screens if the following two prerequisites are completed:

- An AlterPath PM IPDU is connected to an AUX port on the AlterPath OnSite.

  For the procedure, see the *AlterPath OnSite Installation Guide*

- The AUX port is configured for power management.

  For the procedure, see "To Configure an AUX Port for IPDU Power Management [Expert]" on page 266.

Both administrative users and authorized users have access to the first two tabs. The tasks shared by both types of users in the following table with the page numbers where they are documented.

Table 6-2: Power Management Tasks Shared by Authorized Users and Administrative Users

Manage outlets: • View status • Lock / unlock • Power on and off • Cycle • Rename outlets	• "IPDU Power Mgmt.>Outlets Manager [User]" on page 148 • "To View Status, Lock, Unlock, Rename, or Cycle Power Outlets" on page 150
View AlterPath PM IPDU information: • Number of IPDUs • Number of outlets • Whether a buzzer, syslogging, or over current protection is enabled	• "IPDU Power Mgmt.>View IPDUs Info" on page 151 • "To View and Reset IPDU Information [Expert]" on page 153

The following table lists tasks that only administrative users can perform under "IPDU Power Mgmt." with where the tasks are documented.

Table 6-3: Power Managment Configuration Tasks Performed Only by Administrative Users

Configure users to manage power outlets	• "Access>IPDU Power Mgmt.>Users Manager" on page 195 • "To Configure Users to Manage Power Outlets on IPDUs [Expert]" on page 196

Table 6-3: Power Managment Configuration Tasks Performed Only by Administrative Users

Configure names, alarms, logging, and over-current protection for IPDUs.	• "Access>IPDU Power Mgmt.>Configuration" on page 197 • To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]
Upgrade AlterPath PM IPDU information	• "Access>IPDU Power Mgmt.>Software Upgrade" on page 199 • To Upgrade Software on an AlterPath PM [Expert]

Access>IPDU Power Mgmt.>Users Manager

Selecting the "Users Manager" tab under Access>IPDU Power Mgmt. in Expert mode brings up a screen like the one shown in the following figure.

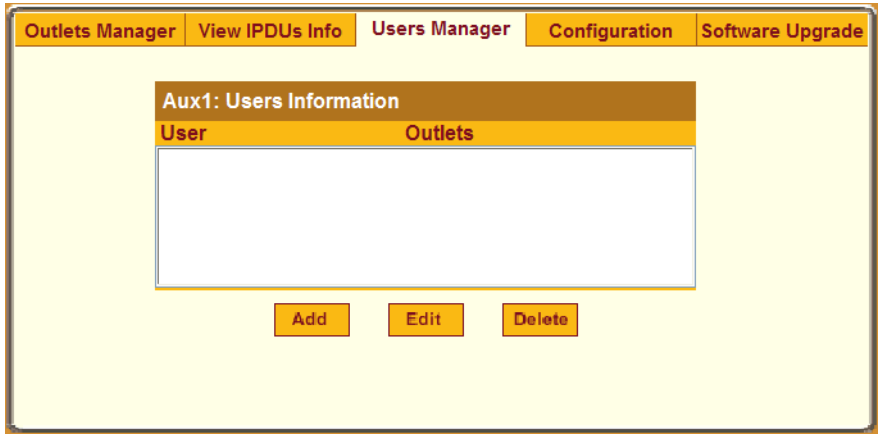


Figure 6-4: Web Manager IPDU Power Mgmt.> Users Manager Screen

An administrative user can use this screen to assign users to outlets. Figure 6-4 shows the screen that displays when a single AlterPath PM IPDU is connected to AUX port 1, which has been configured for power management. The list is empty because no users have been configured for power management.

If more than one port is configured for power management, multiple user lists appear, one for each IPDU power management port.

By default, only administrative users can perform IPDU power management.

Clicking “Add” brings up the following dialog box where the administrative user can specify one or more comma-separated user names and one or more outlets.

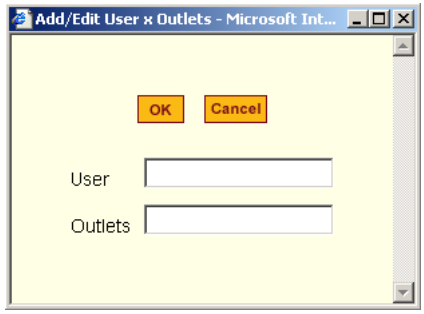
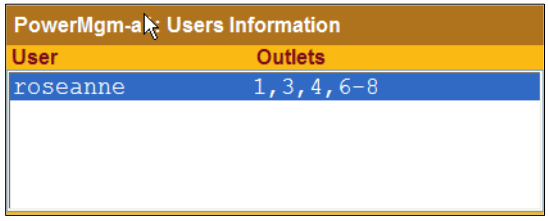


Figure 6-5: IPDU Power Mgmt.>Users Manager “Add User” Dialog Box

A comma can be used to separate outlet numbers, and a hyphen can be used to indicate a range of outlets (for example: 1, 3, 4, 6-8).

When a user is added, the user’s name is added to the list on the Users Manager screen, as shown in the following figure.



▼ *To Configure Users to Manage Power Outlets on IPDUs [Expert]*

1. Go to Access>IPDU Power Mgmt.>Users Manager in Expert mode.

   The “Users Manager” screen appears.

2. To disable a user’s ability to manage power, select the username from the Users Information list and then click “Delete.”

3. To edit a user, select the username from the Users Information list and then click “Edit.”

The “Add/Edit User x Outlets” dialog box appears.

4. To add a new user, click “Add.”

   The “Add/Edit User x Outlets” dialog box appears.

5. In the “Add/Edit User x Outlets” dialog box, do the following as appropriate.

   a. Enter the username in the “User” field.

   b. Enter or modify the numbers of the outlets to which the user is assigned in the “Outlets” field.

6. Click OK.

   The Users Information list displays the changes.

7. Click “apply changes.”

Access>IPDU Power Mgmt.>Configuration

Selecting the “Configuration” tab under Access>IPDU Power Mgmt. in Expert mode brings up a screen like the one shown in the following figure.

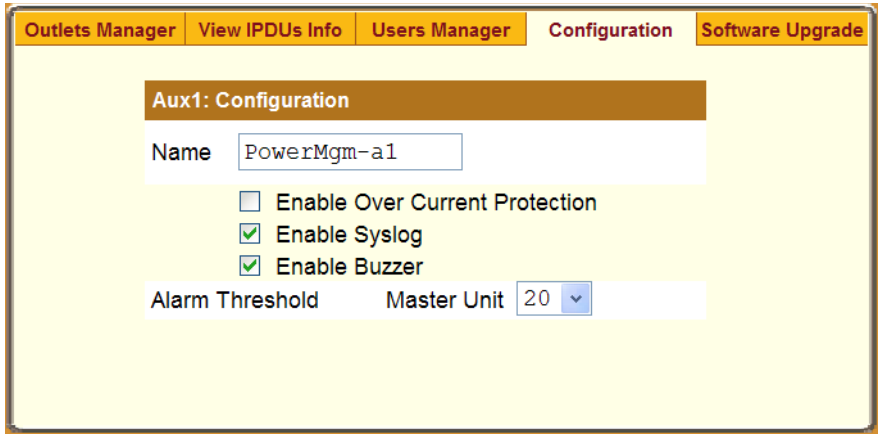


Figure 6-6: Web Manager IPDU Power Management>Configuration Screen

Figure 6-6 shows the Configuration screen when a single AlterPath PM is connected to AUX port 1 and the AUX port is configured for power management. The number of amps shown in the Master Unit pull-down menu

varies according to the model of the connected PM. The figure shows number 20 for a 20 amp PM.

An administrative user can use this screen to specify the following:

- An alias for the IPDU
- A threshold current between 1 and 20 amperes
- Whether any of the following actions occur if the threshold current is exceeded on the IPDU:
  - Whether syslog messages are generated
  - Whether over-current protection is in effect

    If you enable over-current protection, the outlets on the IPDU cannot be turned on if the current on the IPDU exceeds the selected threshold.
  - Whether a buzzer sounds if the current exceeds the defined threshold

The Configuration screen shows an entry for each port that has an AlterPath PM IPDU connected and that is configured for power management. The first connected IPDU is called the *master*, the second and subsequently-connected IPDUs are called *slaves*. On the screen "Master Unit" refers to the first or only connected IPDU. When IPDUs are daisy-chained, the screen displays additional lines to allow you to specify separate thresholds for slave IPDU(s).

▼ To Specify Names, Alarms, Syslogging, and Over-current Protection for IPDUs [Expert]

See "Configuration" on page 142 for background information about the fields on the IPDU Power Mgmt. Configuration screen, if needed.

1. Go to Access>IPDU Power Management>Configuration in Expert mode.
2. The Configuration screen displays entries for all ports configured for power management. Perform the following steps for each IPDU.
   a. If desired, assign an alias to an IPDU in the "Name" field.
   b. For each IPDU, click the appropriate check boxes to enable or disable Over Current Protection, the generation of Syslog files, and the sounding of a Buzzer.

      All of the selected actions occur if a defined threshold is exceeded on the IPDU.

c. If enabling over-current protection, a buzzer, or alarm notification, select an Alarm Threshold from the pull-down menu.

3. Click “apply changes.”

Access>IPDU Power Mgmt.>Software Upgrade

On the “Software Upgrade” screen under Access>IPDU Power Management in Expert mode, an administrative user can upgrade the software on AlterPath PM IPDUs.

The following figure shows the Software Upgrade screen listing the software version on a single AlterPath PM IPDU connected to AUX1.

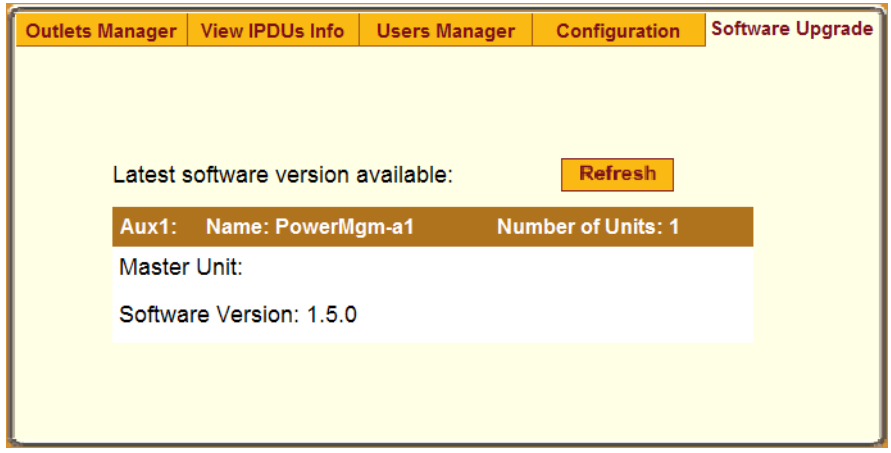


Figure 6-7: Web Manager IPDU Power Management>Software Upgrade Screen

An entry displays for each AUX port configured for power management. The entry displays information about the directly-connected IPDUs, which is called the “master,” and about any daisy-chained IPDUs, which are called “slaves.” The screen displays the version number of the software that is currently installed on each IPDUs.

An administrative user can upgrade IPDU software using this screen, after installing a more-recent version of the AlterPath PM software into the OnSite’s `/tmp` directory with the filename `pmfirmware`. Clicking the “Refresh” button checks for the more-recent version of the PM firmware in the `/tmp/pmfirmware` file. If the `/tmp/pmfirmware` file is present and

the software version it contains is more recent than the installed version, information about the new version is displayed, and an “Update” button appears on the screen.

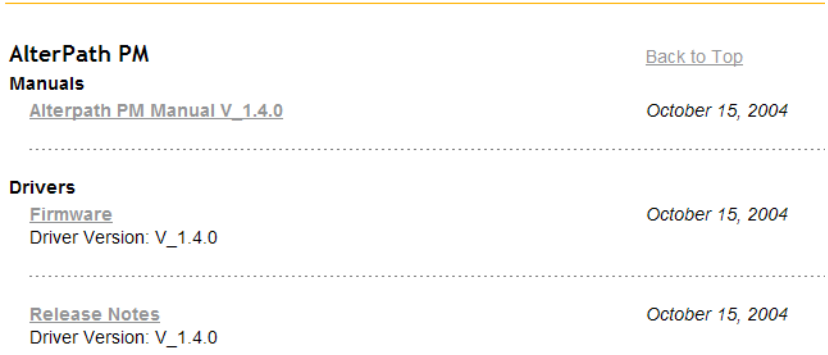
Note: An Upgrade button displays only if a copy of the most-recent firmware has been downloaded into `/tmp/pmfirmware`.

▼ *To Download AlterPath PM Software From Cyclades [Expert]*

An administrative user can use this procedure to download software from the Cyclades website. See “To Upgrade Software on an AlterPath PM [Expert]” on page 201 for how an administrative user can use downloaded AlterPath PM software to update a connected AlterPath PM. While at the website an administrative user can also download updated versions of related documents.

1. On a computer in the same subnet as the OnSite, bring up a browser and go to the download section of the Cyclades website at: http://www.cyclades.com/support/downloads.php.
2. Find the section on the downloads page for the AlterPath PM, and compare the latest driver’s version number to the version shown in the Access>IPDU Power Mgmt.>Software screen.

   The following example shows the “AlterPath PM” section on the downloads page.



For example, the version of AlterPath PM firmware in the previous figure is Driver Version V_1.4.0. You would download it if it is more recent than the version shown on the screen.

3. Click the "Firmware" link.
4. In the version directory, click the name of the binary you want to download.

   For example, `pm_140.bin` is the name of the version 1.4.0 software file.
5. After the download completes, copy the file to the `/tmp` folder with the name `pmfirmware`.

▼ *To Upgrade Software on an AlterPath PM [Expert]*

Perform this procedure to upgrade the software on an AlterPath PM.

This procedure requires the following:

- A more-recent version of the AlterPath PM software than the one shown on the "Software Upgrade" screen is available from Cyclades, Corp.
- You downloaded the more-recent version of the AlterPath PM software and copied it into the OnSite's `/tmp` directory with the filename `pmfirmware`. See "To Download AlterPath PM Software From Cyclades [Expert]" on page 200.

1. Go to Access>IPDU Power Mgmt.>Software Upgrade.

   The Software Upgrade screen displays.
2. Click the Refresh button.

   If a `/tmp/pmfirmware` exists containing a more recent version of the PM software than the one currently installed, an "Update" button appears.
3. Click "Update."
4. Click "apply changes."

Access>IPDU Multi-Outlet Ctrl

A multi-outlet device is a server or other device that has more than one power supply. On the "IPDU Multi-Outlet Ctrl." screen, authorized users can view

and manage the power on a group of outlets that provide power to a server or other device that has multiple power supplies, when the device is connected to a serial port and properly configured.

Selecting the “IPDU Multi-Outlet Ctrl.” option under “Access” in Expert mode brings up the screen shown in the following figure if any of the conditions described on the page are true.

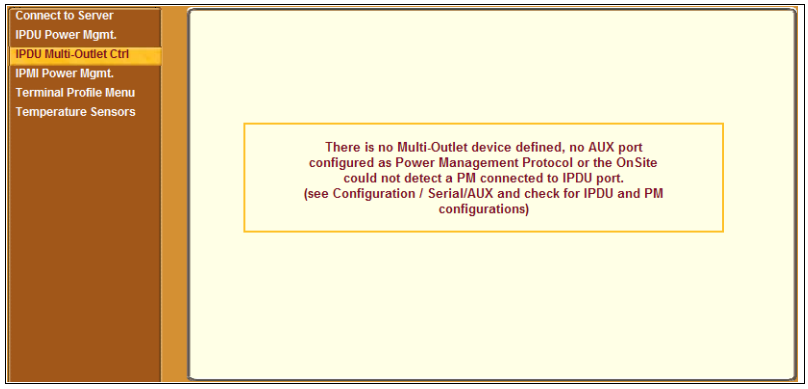


Figure 6-8: Web Manager IPDU Multi-Outlet Ctrl Unconfigured Warning

Selecting the “IPDU Multi-Outlet Ctrl.” option under “Access” in Expert mode brings up the screen shown in the following figure if all the prerequisites listed in Table 6-4, “Tasks for Configuring Multi-Outlet Control,” on page 203 are complete.

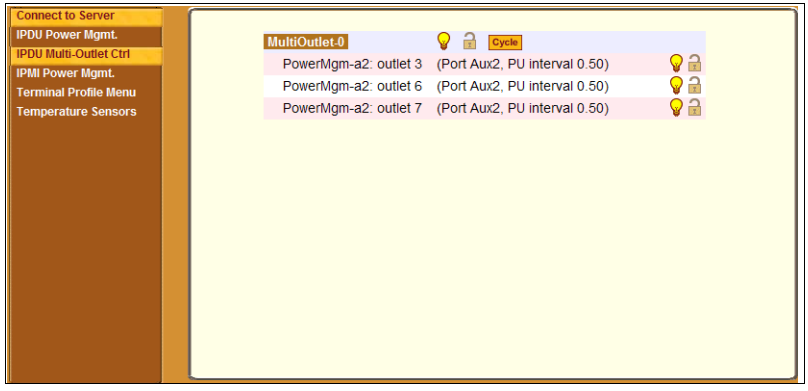


Figure 6-9: Web Manager IPDU Multi-Outlet Ctrl

The multiple outlets do not need to be on the same AlterPath PM IPDU.

Outlets on multiple IPDUs can be managed as a group from this screen.

An administrative user must do the prerequisite tasks shown in the following table before any user can manage power through this screen.

Table 6-4: Tasks for Configuring Multi-Outlet Control

Task	Where Documented
Connect the device that has multiple power supplies to an OnSite serial port and plug it into outlets on one or more AlterPath PM IPDU(s).	N/A
Make sure the IPDU(s) that are powering the device are connected to an AUX port. If the device is plugged into more than one IPDU, the IPDUs should be daisy-chained.	See the *AlterPath OnSite Installation Guide* for how to connect IPDUs to AUX ports.
Configure the AUX port(s) to which the IPDU(s) are connected for power management.	“To Configure an AUX Port for IPDU Power Management [Expert]” on page 266
Configure the multi-outlet device by configuring the serial port to which the device is connected for IPDU power management and define the outlets and the authorized user(s).	“To Configure a Serial Port for IPDU or IPMI Power Management [Expert]” on page 250 “To Configure a User for IPDU Power Management for a Serial Port [Expert]” on page 252

See “Managing Multiple Outlets” on page 154 for how all users manage multiple outlets.

Access>IPMI Power Mgmt.

On the “IPMI Power Mgmt.” screen under “Access” in Expert mode, an administrative user can enable and perform power management of devices that have Intelligent Platform Management Interface (IPMI) management controllers. See “Power Management” on page 35 for an introduction to the options available on the OnSite for IPMI power management, if needed.

As shown in the following figure, if no IPMI devices have been added previously, only the “Add” button appears.

Figure 6-10: Web Manager Access>IPMI Power Mgmt. Screen

When an “Add” button or “Edit” button is pressed, a screen appears for adding or editing a device.

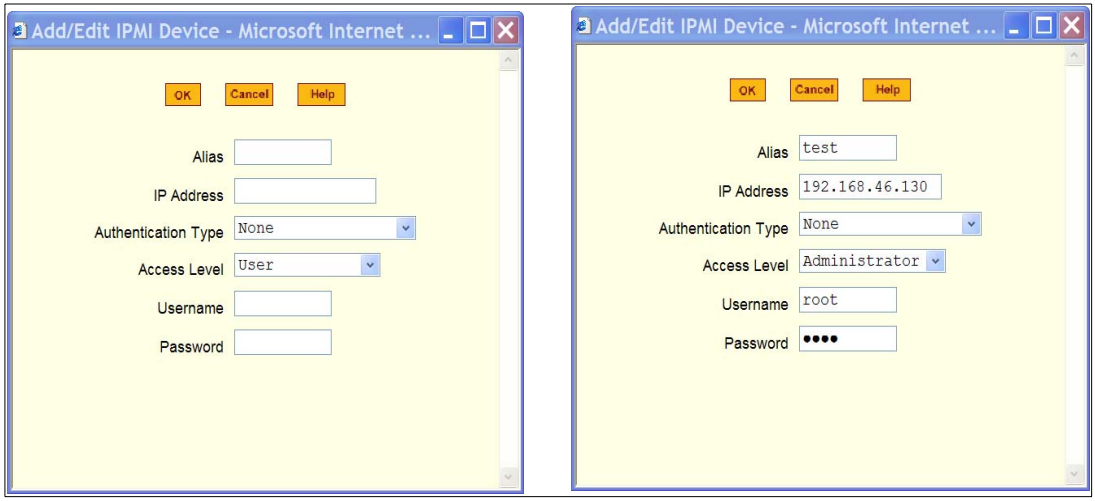


Figure 6-11: Web Manager IPMI Power Mgmt. “Add/Edit IPMI Device” Dialog Boxes

After you fill out the fields or make changes and save the changes, the device is either added to the IPMI Devices list or the configuration for the device is changed. The following figure shows an entry for an IPMI server.

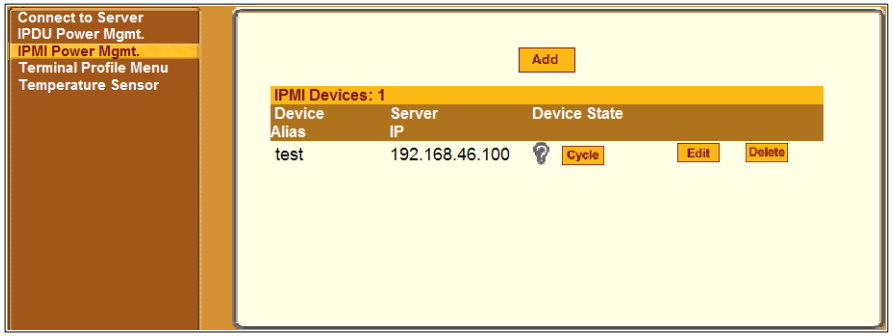


Figure 6-12: Web Manager IPMI Power Mgmt. Example Device Entry

Once an IP address for a device is added to the list of IPMI devices on this screen, any user authorized for power management can turn power on and off and cycle power for the IPMI device through the Web Manager. Also, users authorized to connect to serial ports can perform IPMI power management on a serially-connected device while connected.

Power Management of IPMI devices has the following prerequisites:

- The IPMI device must be available to the OnSite over the network.
- The information in the following table must be obtained from the IPMI device's administrator.

Table 6-5: IPMI Information

Field Name	Description
Device Alias	Optional
IP Address	IP address of the device
Authentication type	None, Straight Password, MD5, MD2
Access Level	(User/Operator/Administrator) Default is User.
Username	Default is NULL user.
Password	Password for administering the remote device

The information is updated in the `/etc/IPMIServer.conf` file.

Selecting the IPMI Power Mgmt. option from the Access menu in Expert mode brings up a screen with all declared IPMI devices, light bulb icons, and the buttons "Add," "Edit," and "Delete."

In the IPMI devices list, light bulb icons indicate the current status of the device. Clicking a light bulb icon toggles the state of the device. When the status is unknown, a question mark appears in the light bulb. A question mark indicates either of the following conditions:

- The device was added or deleted and the changes were not saved.
- The device did not answer IPMI requests.

▼ *To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management [Expert]*

1. Go to Access>IPMI Power Mgmt. in Expert mode.

2. To delete a previously-added IPMI device, select the device's name and then click the "Delete" button.
3. To add a device, click the "Add" button, and perform the following steps.
   a. If desired, enter an optional alias for the device in the "Device Alias:" filed.
   b. Enter the IP address of the IPMI device in the "IP Address:" field.
   c. Choose an authentication type, if desired, from the authentication type pull-down menu.
   d. Choose a user permissions type from the "Access Level" pull-down menu.

      The default is "User."
   e. Enter a Username.
   f. Enter a password for administering the remote device in the "Password" field and go to Step 5.
4. To edit the configuration for a device, click the "Edit" button on the line with the device's name, and make the desired changes on the Edit dialog box.
5. Click OK.
6. Click "save changes."

▼ *To Manage Power on an IPMI Device [Expert]*

1. Go to Access>IPMI Power Mgmt. in Expert mode.

   Entries for all previously-defined IPMI devices appear on the screen. See "To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management [Expert]" on page 206 if needed, for how to add a device.
2. To toggle the state of a device, click the adjacent light bulb icon.
3. To briefly turn the power off then on again, click the "Cycle" button.

Access>Terminal Profile Menu

Selecting the **“**Terminal Profile” option under “Access” in Expert mode brings up a screen like the one shown in the following figure.

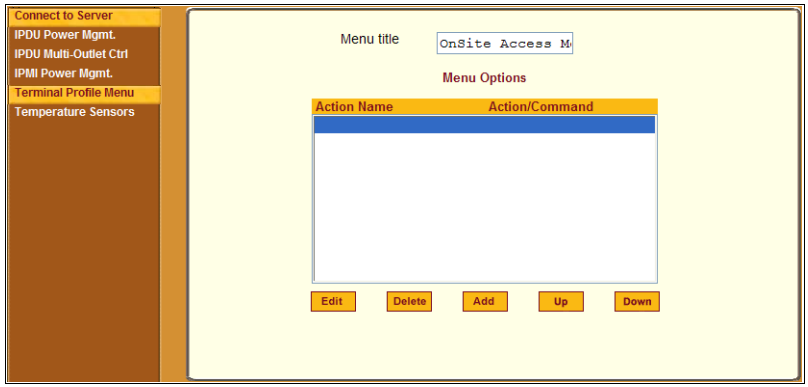


Figure 6-13: Web Manager Access>Terminal Profile Menu Screen

On the screen shown in Figure 6-13, an administrative user can define a terminal command menu to appear when a user turns on a dumb terminal that is connected to one of the serial ports and that is configured as a local terminal. A dumb terminal configured as a local terminal launches a session directly on the OnSite with access to all the Linux commands on the OnSite unless you configure a menu here. The Figure 6-13 shows an empty menu.

The menu can contain any command recognized by the Linux operating system on the OnSite. The most common use of this feature is to create multiple menu options for launching SSH sessions on remote hosts.

When you click “Add,” the “Add Option” dialog box appears, as shown in the following screen example.

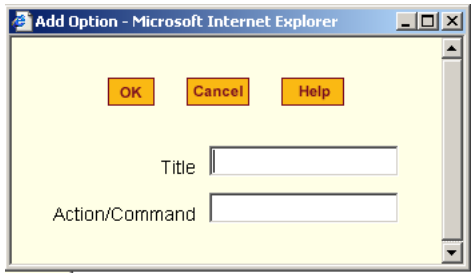


Figure 6-14: Web Manager Terminal Profile Menu “Add Option” Dialog Box

For example, an administrative user can use this screen to create a menu called “SSH to Servers” with options that launch `ssh` connections to several servers, such as shown in the following screen example.

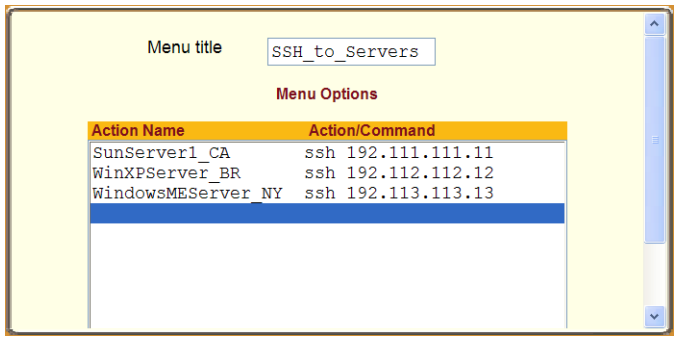


Figure 6-15: Web Manager Terminal Profile Menu Example

▼ *To Create a Menu for a Dumb Terminal [Expert]*

1. Go to Access>Terminal Profile Menu in Expert mode.

   The “Terminal Profile” menu displays.

2. Enter a title for the menu in the “Title” field.
3. To edit an existing menu option, select the action name from the table and then click “Edit.”
4. To add a new menu option, click “Add.”

   The “Add Option” dialog box appears.

a. Enter a title for the menu option in the “Title” field.

b. Enter an action or command to be executed when the user clicks the menu option in the “Action/Command” field, and repeat for the number of options desired.

c. Click OK.

5. Click “apply changes.”

The terminal menu then appears when the dumb terminal is turned on.

Access>Temperature Sensors

OnSite administrative users and regular users can monitor three temperature sensors on the OnSite. The two types of users access the temperature readings from different locations in the Web Manager.

OnSite administrative users can use the “Temperature Sensors” screen under Access in Expert mode to access graphs of temperatures read from the internal temperature sensors. The screen appears as shown in the following figure.

Figure 6-16: Web Manager Temperature Sensor Screen

All users can modify graph display settings, create graph profiles, and apply an existing profile to the current view.

The sensors are located at the following locations within the OnSite:

- FPGA (field programmable gate array)
- Power supply
- CPU

Default and user-added profiles are saved in:
`/new_web/normal/applications/appl/profiles/`

See Table 1-27, “Temperature Graph Parameters,” on page 58 for descriptions of the defaults and allowed values an administrative user can specify to change the display.

For details on how to monitor settings and change graph displays, go to: “To Monitor the OnSite’s Temperature” on page 158.

Configuration

Under “Configuration” in Expert mode, six main options appear in the left menu, as shown in the following figure.

Figure 6-17: Web Manager Configuration Menu Options

See the following sections for details about the tasks performed using the screens under Configuration in Expert mode:

- “Configuration>KVM” on page 212

Configuration>KVM

Selecting Configuration>KVM in Expert mode brings up three KVM options in the left menu as shown in the following figure.

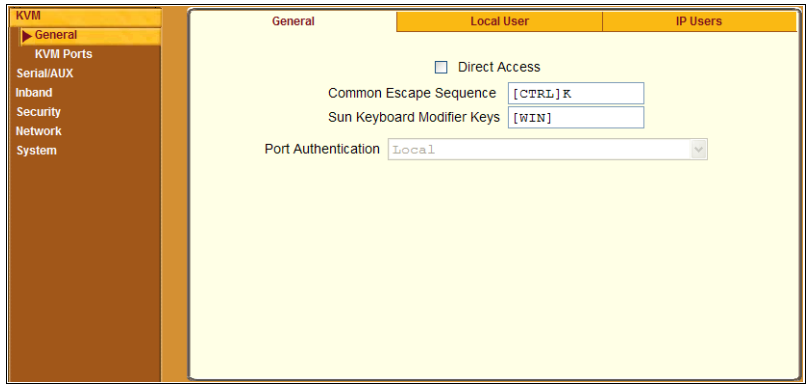


Figure 6-18: Web Manager Configuration>KVM Menu Options

Administrative users can use the KVM menu options for custom configuration of KVM ports.

Configuration>KVM>General

Also as shown in Figure 6-18, selecting Configuration>KVM>General in Expert mode brings up three tabs: General, Local User, and IP Users.

Configuration>KVM>General>General

On the General screen under Configuration>KVM>General in Expert mode, an administrative user can specify the parameters shown in the following table.

Table 6-6: KVM>General>General Screen Fields and Options

Parameter Name	Definition	Where Documented
Direct Access	Selecting this check box enables logins to KVM ports directly from the Web Manager Login screen. **Note:**If the security profile does not permit direct access to KVM ports, this checkbox appears but cannot be selected.	• "Enabling Direct Access to KVM Ports" on page 214 • "To Enable Direct Access to KVM Ports [Expert]" on page 214
Common Escape Sequence	Redefines the escape sequence for KVM connection hot keys.	• "Configuring Keyboard Shortcuts (Hot Keys)" on page 63 • "To Redefine KVM Port Connection Hot Keys [Expert]" on page 215
Sun Keyboard Modifier Keys	Redefines the escape key for Sun keyboard emulation hot keys. If needed, see "Sun Keyboard Emulation Hot Keys" on page 87.	• "Configuring Sun Keyboard Equivalent Hot Keys" on page 64 • "To Redefine the Escape Key for Sun Keyboard Emulation Hot Keys [Expert]" on page 216

Table 6-6: KVM>General>General Screen Fields and Options (Continued)

Parameter Name	Definition	Where Documented
Port Authentication	Allows you to choose whether authentication is required for direct logins to KVM ports. If needed, see the introduction to authentication on the OnSite under "OnSite Authentication Options" on page 7.	• "Configuring Authentication for Direct Access to KVM Ports" on page 216 • "To Configure an Authentication Method for Direct Access to KVM Ports [Expert]" on page 217

Enabling Direct Access to KVM Ports

When direct access to KVM ports is enabled, users authorized to access KVM ports can use a port field on the Web Manager login screen to log in and connect directly to the port. See "To Log Into the Web Manager as admin" on page 108, if desired, for an example of the login screen when direct login is enabled.

▼ To Enable Direct Access to KVM Ports [Expert]

1. Go to Configuration>KVM>General in Expert mode.

   The General screen appears.

2. Click "Direct access."
3. Click "apply changes."

Configuring KVM Port Keyboard Shortcuts (Hot Keys)

An administrative user can use the three KVM General configuration screens (General, Local User, IP Users) to redefine a default set of keyboard shortcuts (called hot keys), which allow users to perform common actions while connected to KVM ports. To perform this optional action, you need to

redefine the common escape sequence portion of each hot key separately from the command key.

The following table summarizes the format of the hot keys, the defaults, and where they can be redefined.

Table 6-7: Format for KVM Port Connection Hot Keys

	Common Escape Sequence	Command Key	Where Defined
Format	"Modifier"+ "*letter key*"	"*letter key*"	Configuration>KVM>General **Note:**The format and valid modifiers are [CTRL], [SHIFT[, [ALT], and [WIN]
Defaults	`Ctrl+k`	`p` to bring up the "power management" screen, `q` to quit, and so forth. See "What You See When Connected to a KVM Port" on page 82 for all the default command keys.	Configuration>KVM>Local Users Configuration>KVM>IP Users

▼ *To Redefine KVM Port Connection Hot Keys [Expert]*

1. Go to Configuration>KVM>General in Expert mode.

   The General screen appears.

2. To redefine the "Common Escape Sequence" enter a key combination starting with a modifier key followed by a letter in all caps, for example, [CTRL]M. Valid modifier keys are [CTRL], [SHIFT[, [ALT], and [WIN].

3. To redefine the command key portion of any AlterPath Viewer keyboard shortcuts, do one of the following steps.

   - To change the command key for users who access KVM ports through the OSD, go to the Local User tab.

   OR

   - To change the command key for users who access KVM ports through the Web Manager (KVM over IP) on OnSite hardware version 1.0.0 go to the IP Users tab.

   AND

   - On the “Local User” or “IP Users” tab, redefine the command keys, as desired, in any of the following fields: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” “Port Info.”

4. Click “apply changes.”

▼ To Redefine the Escape Key for Sun Keyboard Emulation Hot Keys [Expert]

1. Go to Configuration>KVM>General in Expert mode.

   The General screen appears.

2. To redefine the “Sun Keyboard Modifier Keys” replace `[WIN]` with one of the following: `[CTRL]`, `[SHIFT]`, or `[ALT]`.

3. Click “apply changes.”

Configuring Authentication for Direct Access to KVM Ports

Choice of authentication types for direct access to KVM ports are:

- None
- Local
- Kerberos (either Kerberos or Kerberos/DownLocal),
- LDAP (either LDAP or LDAP/DownLocal)
- NTLM (either NTLM Windows NT/2000/2003 or NTLM/DownLocal)

- RADIUS (either RADIUS or RADIUS/DownLocal
- TACACS+ (either TACACS+, and TACACS+/DownLocal)

▼ *To Configure an Authentication Method for Direct Access to KVM Ports [Expert]*

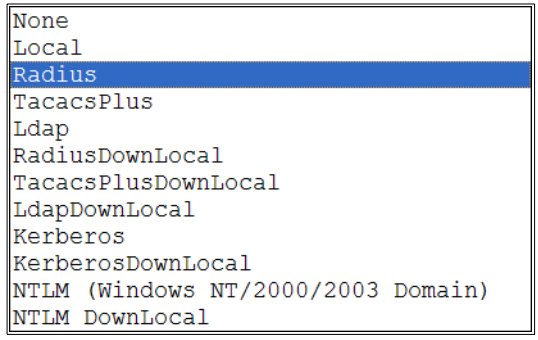
This procedure configures a single authentication method that applies whenever anyone attempts direct access to any KVM port through the Web Manager login screen.

1. Go to Configuration>KVM>General in Expert mode.

   The General screen appears.

2. Select an authentication method from the Authentication pull-down menu.

   The default option is Local.



3. Click “Done.”
4. Click “apply changes.”

   The changes are stored in `/etc/kvmd.conf` on the OnSite.

5. If you select any authentication method other than None or Local, make sure that an authentication server is specified for the selected authentication type.

   See “Configuring Authentication Servers for Logins to the OnSite and Connected Devices” on page 160.

Configuration>KVM>General>Local User

Selecting Configuration>KVM>General>Local User brings up a screen with the fields shown in the following figure.

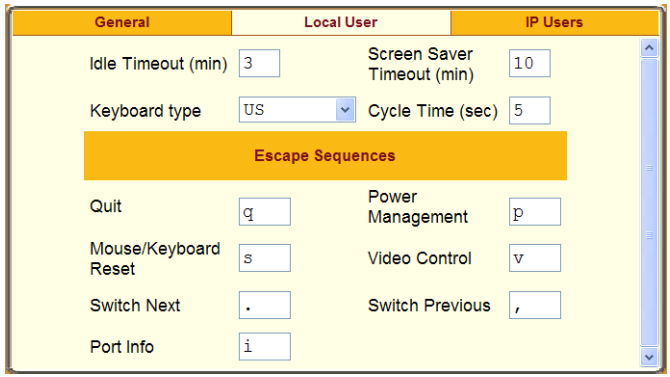


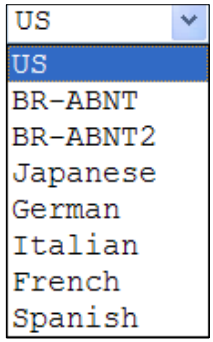
Figure 6-19: Web Manager KVM>General>Local User Screen

On the “Local User” screen under Configuration>KVM>General in Expert mode an administrative user can redefine the default session parameters that apply when a user (called the *Local User*) is directly-connected to the Local User management port on the OnSite and is using the OSD. The following table lists and describes the parameters that appear on the screen.

Table 6-8: Session Parameters for Local User

Field Name	Definition
Idle Timeout	Sets the maximum time (in minutes) for the session to be idle before it is closed.
Screen Save Timeout	Sets the time (in minutes) for the session to be idle before the screen saver activates.

Table 6-8: Session Parameters for Local User (Continued)

Field Name	Definition
Keyboard Type	Sets the keyboard type. Choose the type of keyboard connected to the Local User port on the OnSite. The options from the drop-down list are shown in the following figure. 
Cycle Time	Change the cycle time (in seconds), which is the duration for viewing each server while cycling.
Escape Sequence	Optionally redefine the command key portion of keyboard shortcuts for each type of user. For more information about redefining keyboard shortcuts, see “Configuring Keyboard Shortcuts (Hot Keys)” on page 63 and “To Redefine KVM Port Connection Hot Keys [Expert]” on page 215 if needed.

Configuration>KVM>General>IP Users

On the “IP Users” screen under Configuration>KVM>General in Expert mode, an administrative user can define the default session parameters that apply when a remote user (called the *IP User*) is connected to a KVM port through the Web Manager (in a type of session called *KVM over IP*).

Selecting Configuration>KVM>General>IP Users brings up a screen with the fields shown in the following figure on the OnSite hardware version 1.1.0 or later.

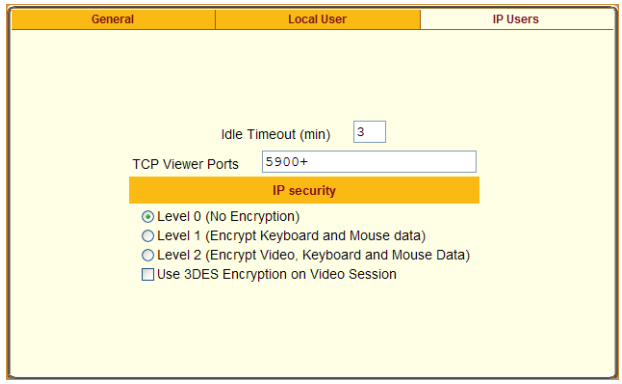


Figure 6-20: Web Manager KVM>General>IP Users Screen, Version 1.1.0

Selecting Configuration>KVM>General>IP Users brings up a screen with the fields shown in the following figure on OnSite hardware version 1.0.0.

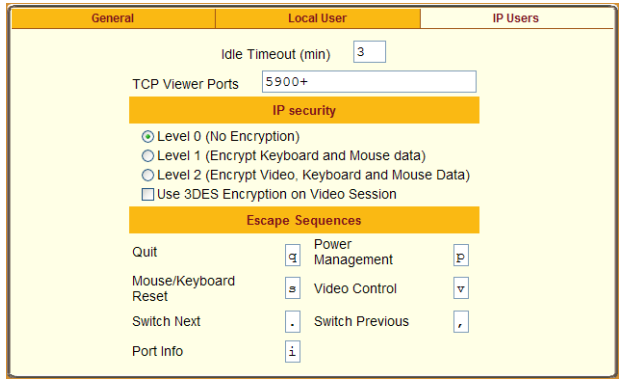


Figure 6-21: Web Manager KVM>General>IP Users Screen, Version 1.0.0

The following table lists and describes the parameters that appear on the screens for both types of users.

Table 6-9: Session Parameters for Local User and IP Users

Field Name	Definition
Idle Timeout	Sets the maximum time (in minutes) for the session to be idle before it is closed.

Table 6-9: Session Parameters for Local User and IP Users (Continued)

Field Name	Definition
TCP Viewer Ports	Change the number of the TCP port used for the AlterPath Viewer. [IP User only.] The default is 5900+. You may need to change the default, for example, if your firewall is blocking port 5900. (For more details, see “Port Numbers and Aliases” on page 47.) Port numbers 1-1024 are reserved. Indicate a range of ports by entering a plus sign (+) after the first port number (as in 2500+) or by entering a dash between two port numbers (as in 2500-2501). Indicate a set of nonadjacent port numbers by separating port numbers with commas (as in 2500, 2508).
IP Security	Specify the level and type of encryption. If the radio buttons for Level 1 or Level 2 are selected, RC4 encryption is used unless the 3DES checkbox is also selected.
Escape Sequence **Note:**This area does not appear when this screen displays on the newest OnSite hardware, because the “Show Connections” menu replaces the hot keys. (See “What You See When Connected to a KVM Port” on page 82.)	Optionally redefine the command key portion of keyboard shortcuts for each type of user. For more information about redefining keyboard shortcuts, see “Configuring Keyboard Shortcuts (Hot Keys)” on page 63 and “To Redefine KVM Port Connection Hot Keys [Expert]” on page 215 if needed.

▼ *To Configure Local User Sessions [Expert]*

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions that are started by a user who is directly logged into the OnSite through a Local User station.

1. Go to Configuration>KVM>General>Local User in Expert mode.
2. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.

3. To change the screen saver timeout, enter a different number of minutes in the “Screen Saver Timeout” field.
4. To change the keyboard type, select a different keyboard from the “Keyboard type” pull-down menu.
5. To change the cycle time, enter a different number of seconds in the “Cycle Time” field.
6. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
7. Click “apply changes.”

▼ *To Configure IP Users (KVM Over IP) Sessions [Expert]*

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a remote user is connected through the Web Manager (in a KVM over IP session).

1. Go to Configuration>KVM>General>IP Users in Expert mode.
2. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.
3. To change the TCP port number used by the AlterPath Viewer, enter another number in the “TCP Viewer Ports” field.
4. Check the radio button next to the desired level or type of encryption.
5. If the “Escape Sequences” area appears on the screen, to optionally change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
6. Click “apply changes.”

KVM Ports

Selecting Configuration>KVM>KVM Ports in Expert mode brings up the screen shown in the following figure.

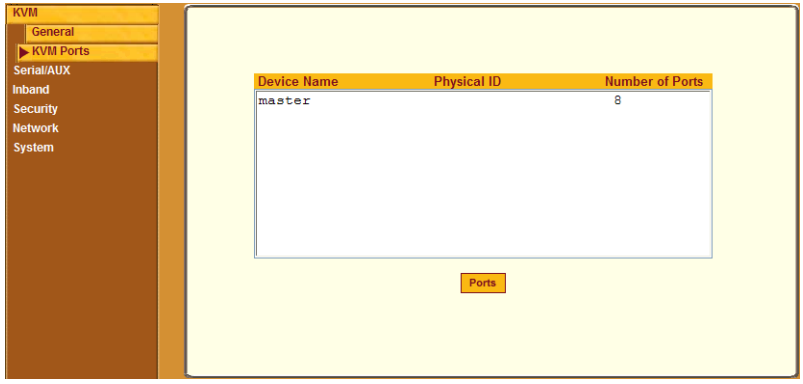


Figure 6-22: Web Manager KVM>KVM Ports Screen

The device name “master” stands for the OnSite. Selecting “master” and clicking the “Ports” button brings up a list of the KVM ports on the OnSite, as shown in the following figure.

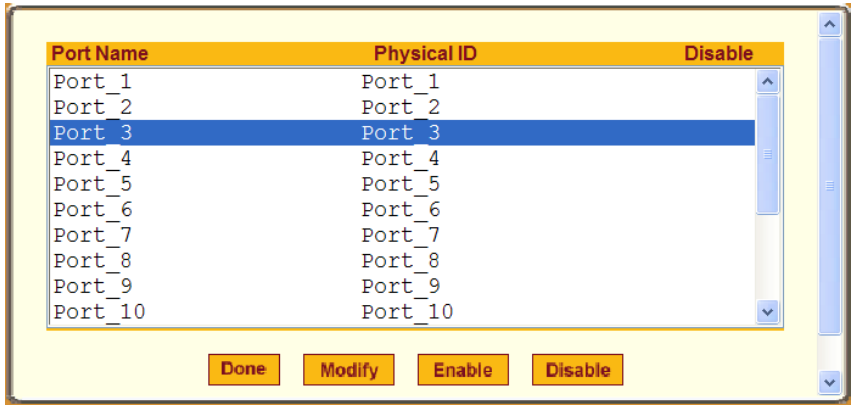


Figure 6-23: KVM Ports List

After selecting one or more ports, the administrative user can enable or disable the KVM port(s) using the “Enable” or “Disable” buttons on the screen.

When you select a port and click the “Modify” button, the dialog box shown in the following figure appears.

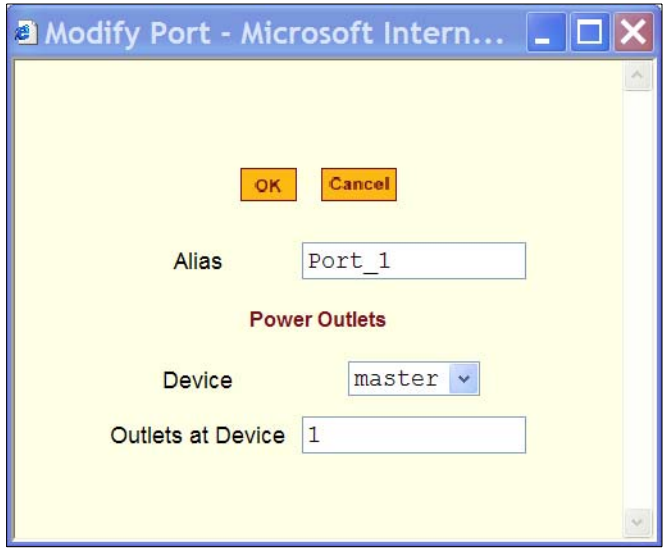


Figure 6-24: KVM “Modify Port” Dialog Box

On the Modify Port dialog box, the administrative user can do the following:

- Configure an alias for a single KVM port
- Configure power management for the server that is connected to the KVM port while the user is logged into the server

Power management while connected to a KVM port is possible only when the following conditions are true:

- The device connected to this port is plugged into an AlterPath PM IPDU that is connected to the AUX1 port on the OnSite
- The AUX1 port is configured for power management.

  See “To Configure an AUX Port for IPDU Power Management [Expert]” on page 266.
- You know the outlet number or numbers into which the server’s power cable or cables are plugged.

Note: On this version of the OnSite, cascading OnSites is not supported. For that reason, the only entry in the Device pull-down list is “master.”

The “Outlets at Device” field is for specifying the number(s) of the outlet(s) into which the device that is connected to the selected KVM port is plugged. Specify multiple outlet numbers separated by commas, or enter a range of numbers separated by a dash. For example, specify outlet number 1,4,6-8 if the device connected to the currently selected KVM port 3 is plugged into outlets 1, 4, 6, 7, and 8 on an IPDU connected to AUX port 1. If more than one IPDU is daisy-chained to a port, the outlet numbers would be specified sequentially. For example, if two IPDUs are daisy-chained, and the first IPDU has eight outlets, then you would enter the number 14 to indicate the sixth outlet on the second IPDU.

▼ *To Configure a KVM Port for Power Management [Expert]*

Perform this procedure to enable a user who is connected to a server through a KVM port to perform power management while connected. When this procedure is completed, the user can manage multiple power outlets for the server while connected to the server.

1. Go to Configuration>KVM >KVM Ports in Expert mode.

   The KVM Ports screen appears.

2. Select the master device or slave devices.
3. Click the “Ports” button.
4. Select a single port to be modified, and then select the “Modify” button.

   The “Modify Port” dialog box appears.

5. Enter the number of one or more outlets into which the server’s power cable is plugged in the “Outlet” field.
6. Click OK on the dialog box.
7. Click “Done” on the screen listing all the ports.
8. Click “apply changes.”

▼ To Configure an Alias for a KVM Port [Expert]

1. Go to Configuration>KVM >KVM Ports in Expert mode, select the device that includes the port(s) you wish to modify.
2. Click the “Ports” button.

   A list of all the selected ports appears.
3. Select a single port to be modified, and then select the “Modify” button.

   The “Modify Port” dialog box appears.
4. To change the port’s alias, do the following steps.
   a. Enter a new alias in the “Alias” field.
   b. Click OK on the dialog box.
5. Click “Done” on the screen listing all the ports.
6. Click “apply changes.”

To Enable or Disable a KVM Port [Expert]

1. Go to Configuration>KVM >KVM Ports in Expert mode, and select the device that contains the port(s) you wish to enable or disable.
2. Click the “Ports” button.
3. A screen listing all the selected ports appears.Select the port(s) to be enabled or disabled, and then select the “Enable” or “Disable” button.
4. Click “Done” on the screen listing all the ports.
5. Click “apply changes.”

Configuration>Serial/AUX

Selecting Configuration>Serial/AUX in Expert mode brings up three options in the left menu, as shown in the following figure.

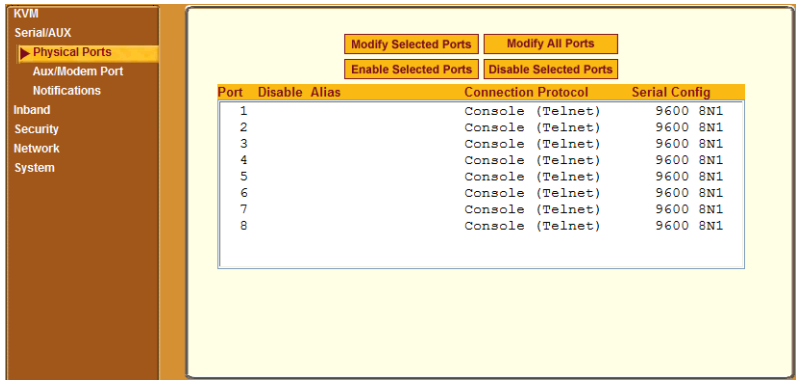


Figure 6-25: Web Manager Configuration>Serial/AUX Menu Options

Using the Serial/AUX menu options as described in the following sections, an administrative user can perform custom configuration of serial and AUX ports.

Configuration>Serial/AUX>Physical Ports

Selecting Physical Ports under Configuration>Serial/AUX in Expert mode, brings up the screen shown in Figure 6-25.

The Physical Ports screen displays a list of the serial ports on the OnSite.

Selecting a port or ports and then clicking the “Modify Selected Ports” button brings up six tabs, as shown in the following figure.

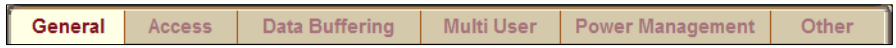


Figure 6-26: Web Manager Serial/AUX>”Modify Selected Ports” Tab Options

By selecting the tabs and bringing up the associated screens, an administrative user can specify a separate set of values for individual serial ports or groups of serial ports or can specify the same set of values for all ports.

See this procedure for how to select ports for modification:

- “To Select One or More Serial Ports [Expert]” on page 193

See the descriptions on how to use the screens in the following sections.

- “Configuration>Serial/AUX>Physical Ports> General” on page 230
- “Configuration>Serial/AUX>Physical Ports> Access” on page 239
- “Configuration>Serial/AUX>Physical Ports>Data Buffering” on page 242
- “Configuration>Serial/AUX>Physical Ports>Multi User” on page 245
- “Configuration>Serial/AUX>Physical Ports>Power Management” on page 247
- “Configuration>Serial/AUX>Physical Ports>Other” on page 253

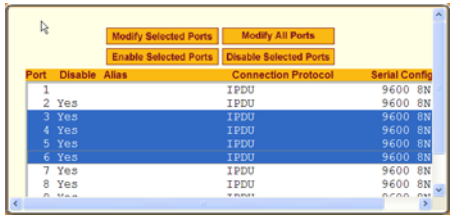
▼ *To Select One or More Serial Ports [Expert]*

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode.

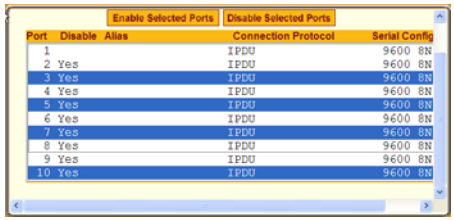
   The Physical Ports screen appears.

2. To select a port or ports, do one of the following steps.

   - To select a single port, click the port.
   - To select multiple ports in a range, click the first port and then hold down the Shift key while selecting another port or ports.



   - To select multiple ports that are not in a range, click the first port and then hold down the Ctrl key while selecting another port.



3. Go to the desired procedure from the following list.

Table 6-10: Configuration Procedures for Selected Serial Ports

▼ *To Enable or Disable Serial Ports [Expert]*

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, select a port or ports to modify.

   If needed, see “To Select One or More Serial Ports [Expert]” on page 193.

2. To enable selected ports, click the “Enable Selected Ports” button.
3. To disable selected ports, click the “Disable Selected Ports” button.
4. Click “Done.”
5. Click “apply changes.”

Configuration>Serial/AUX>Physical Ports> General

Selecting one or more serial ports and clicking either the “Modify Selected Ports” or “Modify all ports” button, brings up a General screen like the one shown in the following figure.

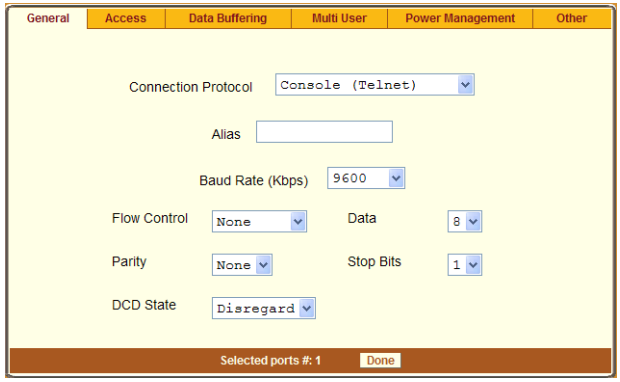


Figure 6-27: Web Manager Serial/AUX>Physical Ports>General Screen

The number(s) of the selected port(s) displays next to the “Done” button at the bottom of the screen in the format: “Selected ports #:*N*,” where *N* stands for the port number.

An administrative user can use the General screen to configure the selected ports. The following table shows the tasks that can be performed using the General screen and provides links to where the tasks are documented.

Table 6-11: Tasks for Configuring Serial Ports (General)

Task	Where Documented
Configure a connection protocol	"Serial/AUX>Physical Ports>General>Console Access Server Protocols" on page 232 "Serial/AUX>Physical Ports>General>Terminal Server Profile Connection Protocols" on page 233 "Serial/AUX>Physical Ports>General>Modem and Power Management Connection Protocols" on page 235
Assign an alias to a single serial port at a time	"To Configure an Alias for a Serial Port [Expert]" on page 238.
Change serial port settings to match the connected device	"To Configure Serial Port Settings to Match the Connected Device [Expert]" on page 238.

Serial/AUX>Physical Ports>General>Console Access Server Protocols

When a serial port is connected to the console port on a device, a Console Access Server (CAS) profile must be defined for the serial port using values you supply in the serial port configuration screens. Selecting the appropriate connection protocol on the Configuration>Serial/AUX>Physical Ports>General Screen is part of defining the CAS profile The connection protocols apply in the following cases:

- When a user accesses the serial port through the Web Manager, the session automatically uses the specified protocol to connect to the console of the connected device.
- When a user logs in remotely over the Internet to the serial port, access is allowed only for the selected protocol. If the user uses another protocol, access is denied. For example, if you specify the “Console (SSH)” protocol, the user can use `ssh` but cannot use `telnet` to access the serial port.

The options from the list of connection protocols in the following table are used when the OnSite serial port is connected to the console port of a server or other device.

Table 6-12: Protocols for Devices With Console Ports Connected to Serial Ports

Protocol Name	Result
Console (Telnet)	Authorized users can use `telnet` to connect to the console of the connected device.
Console (SSH)	Authorized users can use `ssh` to connect to the console of the connected device.
Console (TelnetSSH)	Authorized users can use `telnet` or `SSH` to connect to the console of the connected device. When shared sessions are allowed, simultaneous `telnet` and `SSH` sessions are allowed through the serial port.
Console (Raw)	Authorized users can make a raw socket connection to the console of the connected device.

The remaining serial port connection protocol options are nonstandard, and they should only be used by expert administrators to meet special serial port configuration needs.

Serial/AUX>Physical Ports>General>Terminal Server Profile Connection Protocols

When a dumb terminal is connected to the console port on a device, a Terminal Server (TS) profile must be defined for the serial port using values you supply in the serial port configuration screens. Selecting the appropriate connection protocol on the Configuration>Serial/AUX>Physical Ports>General Screen is part of defining the TS profile. An administrative user can configure serial ports to support dumb terminals in the following two ways:

- Dedicate a dumb terminal to access a single remote server by means of either `telnet`, one of two `ssh` versions, or `raw socket` connections.
- Enable a dumb terminal to access multiple servers and perform any other desired actions through the OnSite.

The TS profile must specify the terminal type, the desired connection protocol, the TCP port number, and the IP address for the remote host (for dedicated dumb terminals). When the user turns on a dedicated dumb terminal, the OnSite starts a session using the specified connection protocol. For example, if “Telnet” is selected as the connection protocol, when the dumb terminal is turned on, the OnSite automatically starts a `telnet` session on the specified host.

The following table describes the connection protocols that can be selected if a dumb terminal is connected to the selected serial port. When you choose one of the dumb terminal connection protocols, TS profile-specific fields appear on the “Other” screen, which you also need to fill out.

Table 6-13: Protocols for Dumb Terminals Connected to Serial Ports

Protocol Name	Result
Telnet	Dedicates a dumb terminal that is connected to the selected serial port to access a specific server using the `telnet` protocol. When the attached dumb terminal is turned on, the OnSite opens a `telnet` session on the server, whose IP address you need to specify on the “Other” screen.

Table 6-13: Protocols for Dumb Terminals Connected to Serial Ports (Continued)

Protocol Name	Result
SSHv1	Dedicates a dumb terminal that is connected to the selected serial port to access a specific server using the `ssh` v1 protocol. When the attached dumb terminal is turned on, the OnSite opens a `SSH` version 1 session on the server, whose IP address you need to specify on the "Other" screen.
SSHv2	Dedicates a dumb terminal that is connected to the selected serial port to access a specific server using the `ssh` v2 protocol. When the attached dumb terminal is turned on, the OnSite opens a `SSH` version 2 session on the server, whose IP address you need to specify on the "Other" screen.
Local Terminal	Dedicates a dumb terminal that is connected to the selected serial port to connect to the OnSite. When the attached dumb terminal is turned on, the OnSite opens a `telnet` session on itself. The user then can use any of the OnSite's Linux commands. An administrative user can also create a Terminal Profile menu (under Access>Terminal Profile Menu in Expert mode) that enables the user to quickly launch sessions on any number of remote hosts.
Raw Socket	Dedicates a dumb terminal that is connected to the selected serial port to access a specific remote host using the `raw socket` protocol. When the attached dumb terminal is turned on, the OnSite opens a `raw socket` session on the host using an IP address and TCP port number you must specify on the "Other" screen.

The following table shows the tasks related to configuring a dumb terminal.

Table 6-14: Tasks for Configuring a Dumb Terminal

Task	Where Documented
Select the appropriate dumb terminal connection protocol	"To Configure a Serial Port Connection Protocol for a Dumb Terminal [Expert]" on page 237

Table 6-14: Tasks for Configuring a Dumb Terminal (Continued)

Task	Where Documented
Complete the TS profile (terminal type, host IP address and TCP port number) as required by the connection protocol	"To Configure Dumb Terminal Server Connection Options [Expert]" on page 255
For a dumb terminal configured with the Local Terminal protocol, configure an optional menu to display when the terminal is turned on and connected to a session on the OnSite	"To Create a Menu for a Dumb Terminal [Expert]" on page 209

Serial/AUX>Physical Ports>General>Modem and Power Management Connection Protocols

The following table shows the connection protocols for modems or AlterPath PM IPDUs connected to the serial ports.

Table 6-15: Protocols for Serial Ports Connected to Modems or IPDUs

Protocol Name	Result
PPP-No Auth	Starts a PPP session without interactive authentication required. Assumes the specified OnSite serial port is connected to an external modem.
PPP	Starts a PPP session with authentication required. Assumes the specified OnSite serial port is connected to an external modem.
SLIP	Starts a SLIP session. Assumes the specified OnSite serial port is connected to an external modem.
CSLIP	Starts a CSLIP session. Assumes the specified OnSite serial port is connected to an external modem.
Power Management	Configures the serial port for power management. Assumes an AlterPath PM IPDU is connected to the serial port.

▼ To Configure a Serial Port Connection Protocol for a Console Connection [Expert]

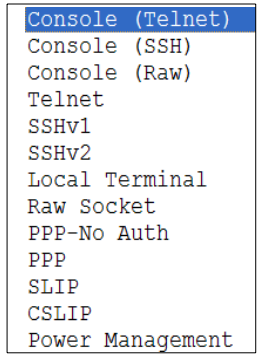
This procedure assumes that the selected serial port is physically connected to a console port on a device.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, select a port or ports to modify, click the appropriate Modify Ports button.

   The General screen appears.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 228.

2. Select one of the three Console options from the Connection Protocol pull-down menu.



   See Table 6-12, "Protocols for Devices With Console Ports Connected to Serial Ports," on page 232, if needed for definitions of the console connection protocols.

3. If you want to change any of the other current settings, go to "To Configure Serial Port Settings to Match the Connected Device [Expert]" on page 238.

4. If you are finished, click "Done."

▼ To Configure a Serial Port Connection Protocol for a Dumb Terminal [Expert]

This procedure assumes that the selected serial port is physically connected to a dumb terminal. See Table 6-13, “Protocols for Dumb Terminals Connected to Serial Ports,” on page 233, if needed for definitions of the dumb terminal connection protocols.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, select a port or ports to modify, click the appropriate Modify Ports button.

   The General screen appears.

   If needed, see “To Select One or More Serial Ports [Expert]” on page 228.

2. To configure a dumb terminal to automatically connect to the OnSite, do the following steps.

   a. Select “Local Terminal” from the “Connection Protocol” pull-down menu.

   b. Define a terminal profile menu, if desired.

      Go to “To Create a Menu for a Dumb Terminal [Expert]” on page 209.

3. To configure a dedicated dumb terminal to automatically connect to a server, do the following steps.

   a. Select “Telnet,” “SSHv1,” “SSHv2,” or “Raw Socket” from the “Connection Protocol” pull-down menu.

   b. Specify the terminal type and the address of the remote host using the “Other” screen.

      Go to “To Configure Dumb Terminal Server Connection Options [Expert]” on page 255.

4. If you want to change any of the settings, go to “To Configure Serial Port Settings to Match the Connected Device [Expert]” on page 238.

5. If you are finished, click “Done.”

▼ To Configure an Alias for a Serial Port [Expert]

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, select a port to modify, and click the Modify Ports button.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   The General screen appears. The Alias field appears on the General screen only when a single port is selected for modification.

2. Enter the desired string in the Alias field.
3. Click "Done."
4. Click "apply changes."

▼ To Configure Serial Port Settings to Match the Connected Device [Expert]

The settings for a serial port must match the connection settings on the connected device. The default settings are correct for most devices. If the connection does not work, you might have to experiment with changing these settings. Check the device's manual if possible to see what the device's settings are.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   The General screen appears.

2. To change the baud rate, select an option from 2400 to 921600 Kbps from the Baud Rate pull-down menu.

   The default is 9600, which is the most common baud rate for serially-managed devices.

3. To change the flow control, select None, Hardware, or Software from the Flow Control pull-down menu.

   The default is None.

4. To change the parity, select None, Odd, or Even from the Parity pull-down menu.

The default is None.

5. To change the data size, select an option from 5 to 8 from the Data pull-down menu.

   The default is 8.

6. To change the stop bits, select 1 or 2 from the stop bits pull-down menu.

   The default is 1.

7. To change whether the data carrier detect (DCD) state is disregarded or not, select either “Disregard” or “Regard.”

8. Click “Done.”

9. Click “apply changes.”

Configuration>Serial/AUX>Physical Ports> Access

Selecting Configuration>Serial/AUX>Physical Ports in Expert Mode, selecting one or more serial ports, and then selecting the Access tab, brings up a screen like the one shown in the following figure.

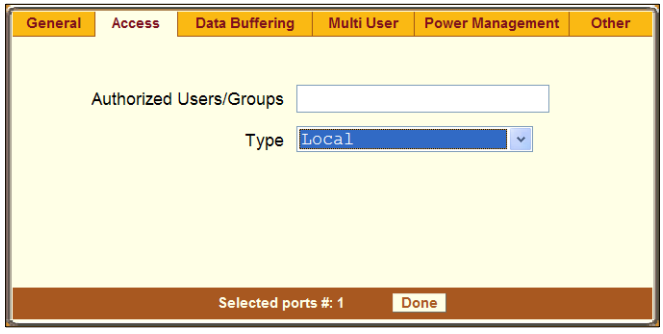


Figure 6-28: Web Manager Serial/AUX>Physical Ports>Access Screen

On the Access screen under Configuration>Serial/AUX>Physical Ports in Expert mode, an administrative user can perform the tasks shown in the following table.

Table 6-16: Tasks Performed Using the Serial/AUX> Physical Ports>Access Screen

Task	Notes and Where Documented
Restrict access to a serial port by specifying one or more users or groups (and thereby excluding all others) or by denying access to one or more users or groups	The default is all users have access. See "To Configure User Access for One or More Serial Ports [Expert]" on page 200
Choose an authentication type for the serial port from the following pull-down list.	The default is no authentication (authentication type=None). See "OnSite Authentication Options" on page 7, if needed for more details. For the procedure, see "To Configure an Authentication Method for Logins Through a Serial Port [Expert]" on page 201.

Access can be denied to one or more users or groups by entering an exclamation point (!) before the user or group name. For example, to explicitly deny access to a user called "noadmin," and enable access only to a single user called "manuel," you would enter the following:

```
!noadmin,manuel
```

Note that the names are separated by a comma.

▼ *To Configure Serial Port Access for Users [Expert]*

Use this procedure if you want to specify a list of authorized users or groups and deny access to all other users and groups.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   Six tabs appear.

2. Click the Access tab.

The Access screen appears.

3. To restrict access to one or more users or to a group of users, enter previously defined user or group names in the "Authorized Users/Groups" field, with the names separated by commas.
4. To deny access to one or more users or groups, preface the user or group names with an exclamation point (!).
5. Click "Done."
6. Click "apply changes."

▼ *To Configure a Serial Port Authentication Method [Expert]*

This procedure configures an authentication method that applies to logins to serial ports. Different methods can be selected for individual ports or for groups of ports.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   Six tabs appear.
2. Click the Access tab.
3. To select an authentication method, select one of the options in the Type menu.
4. Click "Done."
5. Click "apply changes."

   The changes are stored in `/etc/portslave/pslave.conf` on the OnSite.
6. Make sure that an authentication server is specified for the selected authentication type.

   See "Tasks for Setting up Authentication Servers for Each Authentication Method" on page 278 for links to the procedures that apply to each authentication method.

Configuration>Serial/AUX>Physical Ports>Data Buffering

Selecting Configuration>Serial/AUX>Physical Ports in Expert Mode, selecting one or more serial ports, and then selecting the Data Buffering tab, brings up a screen like the one shown in the following figure.

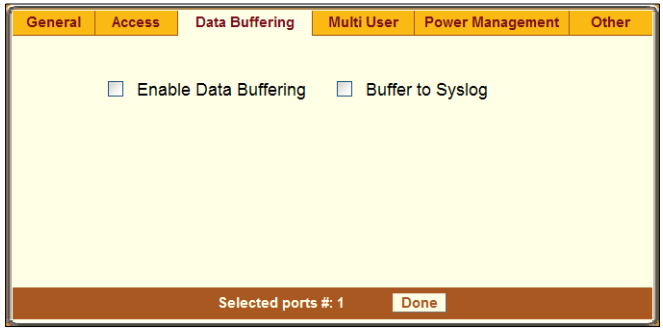


Figure 6-29: Web Manager Serial/AUX>Physical Ports>Data Buffering Screen

An administrative user can select one or more serial ports and then use this screen to configure data buffering for the selected port(s).

This screen displays different fields depending on whether one or both checkboxes are checked. The screen shown in the previous figure displays only the “Enable Data Buffering” and “Buffer to Syslog” items with adjacent checkboxes not checked.

If “Enable Data Buffering” is checked, the screen displays different fields depending on whether “Local” or “Remote” are selected from the “Destination” menu.

If “Buffer to Syslog” is checked, data buffer files are sent to the syslog server. The syslog server must be previously configured. Get the IP address of the syslog server from the server’s administrator, and make sure the syslog server has been configured as described under “To Add a Syslog Server [Wizard]” on page 126.

The following screen shows both checkboxes (“Enable Data Buffering” and “Buffer to Syslog”) and the “Local” destination selected.

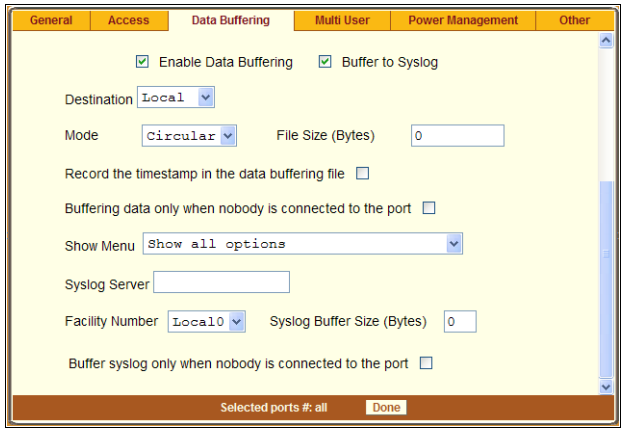


Figure 6-30: Web Manager Serial/AUX>Physical Ports>Data Buffering Fields and Menu Options

▼ *To Configure Data Buffering for Serial Ports [Expert]*

To configure data buffer files to be stored remotely, make sure that a system administrator has already configured an NFS server and shared the mount point. Obtain the facility number for the OnSite from the system administrator of the syslog server. Options range from Local10 to Local17. See “Notifications, Alarms, and Data Buffering” on page 40 for how the facility number is used, if needed.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see “To Select One or More Serial Ports [Expert]” on page 193.

   Six tabs appear.

2. Select the Data Buffering tab.

   The Data Buffering screen displays.

3. Check either or both of the checkboxes.

4. If you selected “Enable Data Buffering,” perform the following steps.

a. From the “Destination” pull-down menu, choose “Local” or “Remote” to specify whether the data buffer files are stored locally or on a file server.

b. If you chose “Local” from the “Destination” pull-down menu, do the following:

i. Choose “Circular” or “Linear” from the “Mode” pull-down menu.

ii. Enter a size larger than 0 in the “File Size (Bytes) field.

c. If you chose “Remote” from the “Destination” pull-down menu, enter the NFS mount point for the directory where data buffer file is to be stored in the “NFS File Path” field.

d. Click the checkbox next to “Record the timestamp in the data buffering file” to specify whether to include a timestamp with the data.

e. From the “Show Menu” pull-down menu, choose among the following options:

- Show all options
- No
- Show data buffering file only
- Show without the erase options

f. If you do not want to configure buffering to a syslog server, go to Step 6.

5. If you checked “Buffer to Syslog,” perform the following steps.

a. Enter the IP address of the syslog server in the “Syslog Server” field.

b. Choose an option from the “Facility Number” pull-down menu.

c. Enter the maximum size of the buffer in the “Syslog Buffer Size” field.

d. Click the radio button next to one of the following options:

- Buffer Syslog at all times
- Buffer only when nobody is connected to the port

6. Click “Done.”

7. Click “apply changes.”

To configure alarm notifications to be sent based on the type of buffered data, see “To Choose a Method for Sending Notifications for Serial Port Data Buffering Events [Expert]” on page 270.

Configuration>Serial/AUX>Physical Ports>Multi User

Selecting Configuration>Serial/AUX>Physical Ports in Expert Mode, selecting one or more serial ports, and then selecting the Multi User tab brings up a screen like the one shown in the following figure.

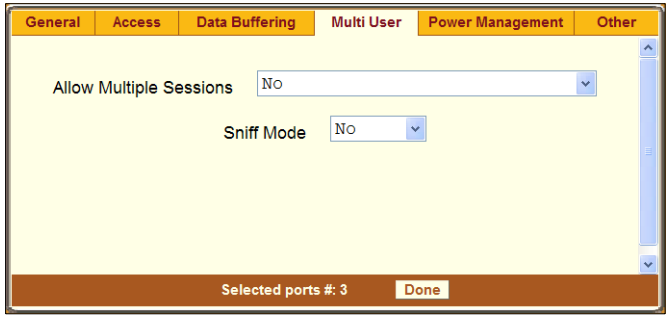


Figure 6-31: Web Manager Configuration>Serial/AUX>Physical Ports>Multi User Screen

The administrative user can use this screen to allow multiple users to connect to a serial port at the same time and allow or disallow port sharing (simultaneous access to the same port). To connect to the port or start a shared session at the port, the user must have permission to access the port.

The following table describes the options from the “Allow Multiple Sessions” pull-down menu.

Table 6-17: Options on the “Allow Multiple Sessions” Menu

Menu Option	Description
No	Only one shared session and one normal session are allowed. The shared session menu is presented.

Table 6-17: Options on the "Allow Multiple Sessions" Menu (Continued)

Menu Option	Description
Yes (show menu)	Multiple read/write sessions and multiple shared (read-only) sessions are allowed. The multiple shared session menu is presented.
Read/Write (do not show menu)	Read/write sessions are opened without a shared session menu being presented
ReadOnly (do not show menu)	Read only sessions are opened without a shared session menu being presented.

The "Sniff Mode" pull-down menu options "Out," "In," "In/Out," and "No" configure the type of data that displays on the monitor.

▼ *To Configure Multiple Serial Port Sessions and Port Sharing [Expert]*

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   Six tabs appear.

2. Click the "Multi User" tab.
3. To allow or to prevent multiple sessions, select an option from the "Allow Multiple Sessions" pull-down menu.

   The options are: "No," "Yes (show menu)," "Read/Write (do not show menu)," "ReadOnly."

4. To configure the type of data that displays on the monitor in a port-sharing session, select an option from the "Sniff Mode" pull-down menu.
5. Click "Done."
6. Click "apply changes."

Configuration>Serial/AUX>Physical Ports>Power Management

Selecting Configuration>Serial/AUX>Physical Ports in Expert Mode, selecting one or more serial ports, and then selecting the Power Management tab, brings up a screen like the one shown in the following figure.

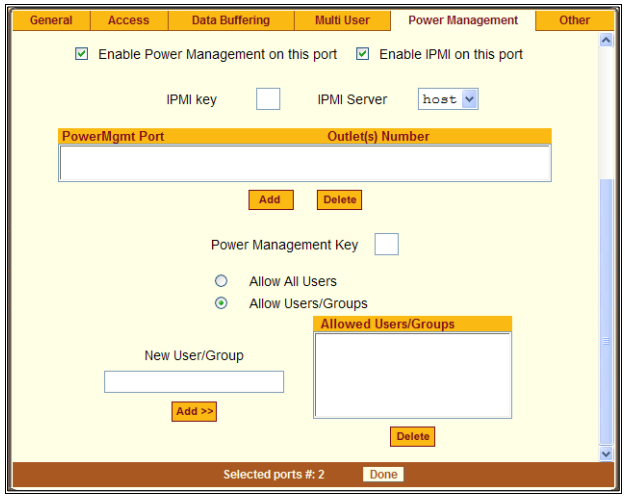


Figure 6-32: Web Manager Configuration>Serial/AUX>Physical Ports>Power Management Screen

The administrative user can use this screen to authorize one or more users to perform either IPDU or IPMI power management on a device that is connected to the selected serial port. While connected to the device, an authorized user can enter a hot key to bring up a menu or a dialog box to perform IPDU or IPMI power managment. While logged into the Web Manager, the authorized user can perform IPDU power management through the “IPDU Multi-Outlet Ctrl” screen.

Note: “Enable power management” on this screen refers to IPDU power management.

Configuring either IPDU or IPMI power management requires you to specify a hot key. The default for IPDU power management is `Ctrl+p`. The default for IPMI power management is `Ctrl+Shift+i`.

Note: The checkbox next to “Enable IPMI on this port” cannot be checked unless an OnSite administrator has previously configured an IPMI server as described under Access>IPMI Power Mgmt.

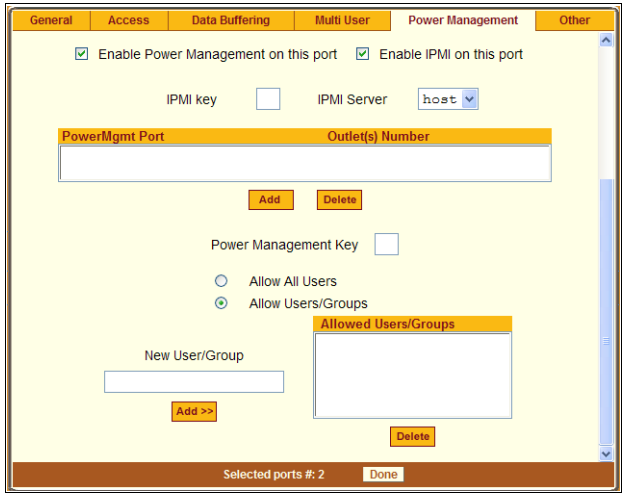


Figure 6-33: Web Manager Configuration>Serial/AUX>Physical Ports>Power Management Options

If only “Enable Power Management on this port” is selected, the “IPMI key” and “IPMI Server” menu do not appear. If only “Enable IPMI on this port” is checked, only the “IPMI key” and “IPMI Server” menu appear.

Power management while connected to a port is possible only when one or both of the following conditions are true

- IPDU power management can be configured when the device connected to this serial port is plugged into one or more outlets on an AlterPath PM IPDU that is connected to an AUX port on the OnSite, and the AUX port is configured for power management.

  See “To Configure an AUX Port for IPDU Power Management [Expert]” on page 266.

- IPMI power management can be configured when the device connected to this serial port is a server with an IPMI controller, and the server is listed in the “IPMI Server” list that appears on this screen when the “Enable IPMI on this port” checkbox has been checked.

  To be listed in the “IPMI Server” list, the server must have been previously configured as described in “To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management [Expert]” on page 206.

If you click “Enable power management” and click the “Add” button, the “Add Outlet” dialog box appears, as shown in the following figure. In the dialog box, an administrative user can specify the AlterPath PM IPDU and the outlet number(s) into which the device is plugged.

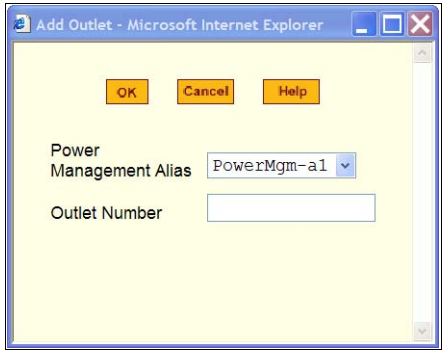


Figure 6-34: Web Manager Configuration>Serial/AUX>Physical Ports>Power Management>Add Outlets Dialog Box

The “PowerMgm-a1 item” on the “Power Management Alias” pull-down menu in the example figure indicates that an IPDU is connected to AUX port a1, which is configured for power management. If more than one IPDU is listed in the “Power Management Alias” pull-down menu, more than one AUX port on the OnSite is connected to an IPDU and configured for power management.

The “Outlet Number” field is for entering the number(s) of the outlet(s) into which the device that is connected to the selected serial port is plugged. Enter outlet numbers separated by commas, or enter a range of numbers separated by a dash. For example, you could specify outlet number 1,4,5-8 as shown in the following figure, if the device connected to the currently selected serial

port 3 is plugged into outlets 1, 4, 5, 6, 7, and 8 on an IPDU connected to AUX port 1.

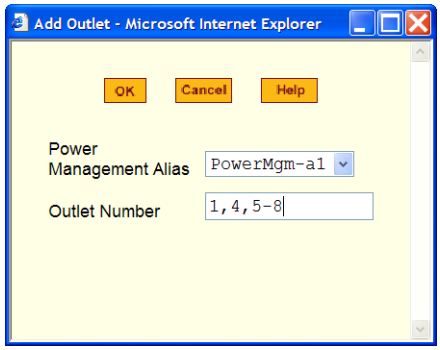


Figure 6-35: Web Manager Configuration>Serial/AUX>Physical Ports>Power Management—Add Outlets Example

If more than one IPDU is daisy-chained to a port configured for power management, the outlet numbers are specified sequentially. For example, if two IPDUs are daisy-chained, and the first IPDU has eight outlets, then you would enter the number 14 to indicate the sixth outlet on the second IPDU.

▼ *To Configure a Serial Port for IPDU or IPMI Power Management [Expert]*

This procedure assumes the prerequisites described in "Configuration>Serial/AUX>Physical Ports>Power Management" on page 247 are completed. Perform this procedure to enable power management of a device that is connected to a serial port when that device is plugged into one or more outlets on an AlterPath PM IPDU that is connected to an AUX port on the OnSite and properly configured.

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see "To Select One or More Serial Ports [Expert]" on page 193.

   Six tabs appear.

2. Click the "Power Management" tab.

3. To enable Power Management of a device connected to the current port and plugged into a connected IPDU, click “Enable Power Management on this port.” and perform the following steps.

   a. Click the “Add” button.

      The “Add Outlet” dialog box appears.

   b. Enter the outlet number(s) into which the device connected to the selected port is plugged.

   c. Click OK.

      The power management port and the specified outlet numbers display on the PowerMgmt Port list.

   d. Enter the power management hot key in the “Power Management Key” field.

      Enter a caret (^) for the escape key, as in `^p`. The caret stands for the `Ctrl` key.

   - If you want to configure IPMI power management on this port, continue to Step 4.
   - If you are done, go to Step 5.

4. To enable IPMI Power Management of an IPMI device connected to the currently-selected port, do the following steps.

   a. Check the checkbox next to “Enable IPMI on this port.”

      The “IPMI key” and “IPMI Server” fields appear.

   b. Optional: change the IPMI hot key.

      Enter the key combination in the IPMI key field with `^`, as in `^i`. The caret (^) stands for the `Ctrl` key.

      A user of the device connected to this serial port can use this hot key to bring up the IPMI power management screen while connected to the port as described in “To Manage Power While Connected to a Serial Port” on page 106.

   c. Select the name of the previously-added IPMI device from the “IPMI Server” pull-down menu.

5. Click “Done.”

6. Click “apply changes.”

▼ To Configure a User for IPDU Power Management for a Serial Port [Expert]

Perform this procedure to authorize a user to perform power management for a device that is connected to one of the OnSite’s serial ports. The device must be plugged into one or more outlets on an AlterPath PM IPDU that is connected to one of the AUX ports, and the AUX port must be configured for power management. A user configured for IPDU power management for a serial port can manage power for the device connected to the serial port in the two following ways:

- While connected to the device through the serial port(s)
- Through the Web Manager’s “IPDU Multi-Outlet Ctrl.” screen

1. Configure the serial port for IPDU power management as described in Step 1. through Step 3. under “To Configure a Serial Port for IPDU or IPMI Power Management [Expert]” on page 208, but do not click the “Done” button.
2. To allow everyone with access permissions for this port to perform power management on this port, click the “Allow All Users” radio button.
3. To restrict power management on this port to a restricted list of users authorized to access this port, click the “Allow Users/Groups.”
4. Enter a valid username or groupname in the “New User/Group” field, and click “Add.”
5. Click “Done.”
6. Click “apply changes.”

Configuration>Serial/AUX>Physical Ports>Other

Selecting Configuration>Serial/AUX>Physical Ports in Expert Mode, selecting one or more serial ports, and then selecting the Other tab, brings up a screen like the one shown in the following figure.

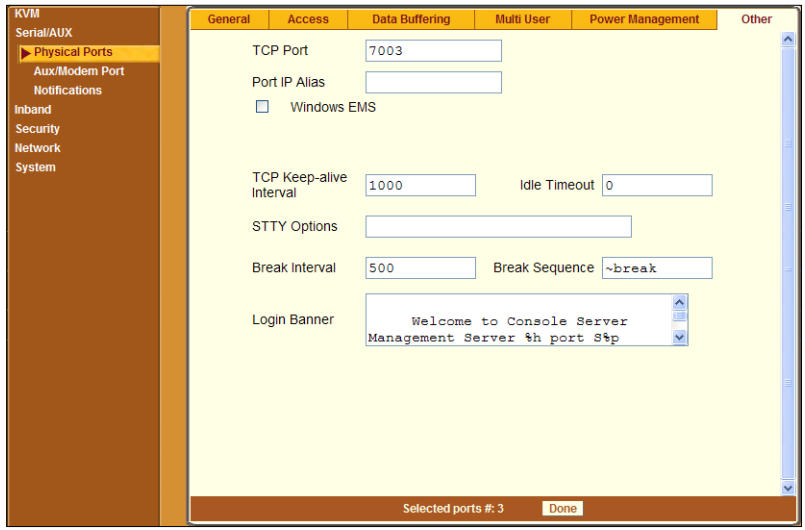


Figure 6-36: Web Manager Configuration>Serial/AUX>Physical Ports> Other Screen

An administrative user can use this screen to configure a non-default TCP port, a port IP alias, TCP keep-alive interval, idle timeout, stty options, break interval, break sequence, and login banner for a serial port. An administrative user can also configure a remote host for a dumb terminal to access and the terminal types for a connected dumb terminal.

Note: Some Sun servers are designed to switch to monitor mode when they receive a break signal on the console port, which allows the system administrator to reset, reboot, or reconfigure the server in the case of a system lockup. To reduce the risk of false breaks bringing down that kind of server, an administrative user can define the break signal as a sequence of ASCII characters that are not likely to be accidentally generated.

When one of the dumb terminal connection options in the General screen is selected (see Table 6-13, “Protocols for Dumb Terminals Connected to Serial Ports,” on page 233), additional fields appear on this screen and some fields disappear, as shown in the following figure.

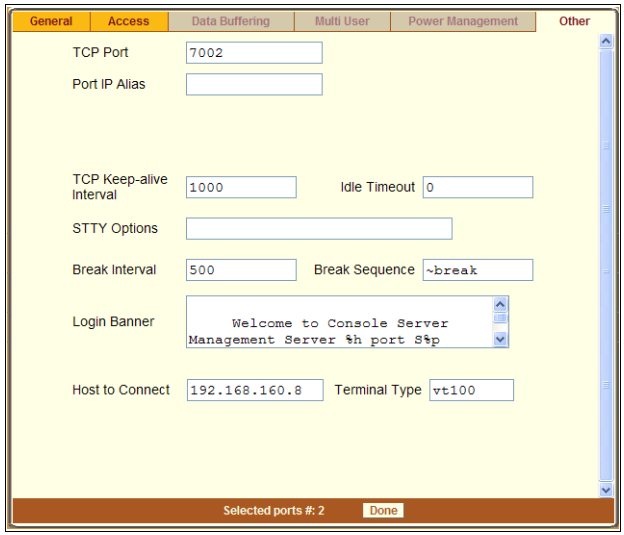


Figure 6-37: Web Manager Configuration>Serial/AUX>Physical Ports>General Screen—Other Screen When Terminal Protocol is Selected

For dumb terminals dedicated to remote servers you need to specify a host IP address in the “Host to Connect” field. For any type of dumb terminal, you need to enter the type of terminal in the “Terminal Type” field.

▼ *To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console [Expert]*

1. Go to Configuration>Serial/AUX>Physical Ports in Expert mode, and select a port or ports to modify.

   If needed, see “To Select One or More Serial Ports [Expert]” on page 193.

   Six tabs appear.

2. Select the “Other” tab.

   The Other screen appears.

3. To change the port number for the serial port, enter another number in the “TCP Port” field.

4. To assign a name to the port’s IP address, enter an alias in the “Port IP Alias” field. For example, if the serial port is connected to a CISCO router, you could assign it a name like “cisco_router1.”

5. If connecting to a server running the Microsoft Windows Server 2003 operating system through the emergency management services (EMS) console, check the “Windows EMS” checkbox.

6. To change the keep-alive interval, enter another number in the “TCP Keep-alive Interval” field.

7. To change the idle timeout interval, enter another value in the “Idle Timeout” field.

8. Specify stty options, if desired, in the “STTY Options” field.

9. To change the break interval, enter a new number in the “Break Interval” field.

10. To change the break sequence, enter a new sequence in the “Break Sequence” field.

11. To change the content of the login banner, enter new content in the “Login Banner” field.

12. Click “Done.”

13. Click “apply changes.”

▼ *To Configure Dumb Terminal Server Connection Options [Expert]*

Do this procedure if you have connected a dumb terminal to a serial port.

1. Select the port and choose an appropriate connection protocol from the General screen.

   See Table 6-13, “Protocols for Dumb Terminals Connected to Serial Ports,” on page 233 and “To Configure a Serial Port Connection Protocol for a Console Connection [Expert]” on page 236).

When one of the dumb terminal connection protocols are selected three tabs are greyed out of the six Serial/AUX>Physical Ports>[Select a serial port] tabs.

2. Select the “Other” tab.

   The Other screen appears.

3. To change the port number used to access the serial port, enter another number in the “TCP Port” field.
4. To change the keep-alive interval, enter another number in the “TCP Keep-alive Interval” field.
5. To change the idle timeout interval, enter another value in the “Idle Timeout” field.
6. Specify stty options, if desired, in the “STTY Options” field.
7. To change the break interval, enter a new number in the “Break Interval” field.
8. To change the break sequence, enter a new sequence in the “Break Sequence” field.
9. To change the content of the login banner, enter new content in the “Login Banner” field.
10. For a dedicated dumb terminal, enter the IP address of the desired host in the “Host to Connect” field.
11. Enter the type of terminal in the “Terminal Type” field.
12. Click “Done.”
13. Click “apply changes.”

Configuration>Serial/AUX>Aux/Modem Port

Selecting Configuration>Serial/AUX>Aux/Modem Port in Expert mode brings up three tabs, as shown in the following figure.

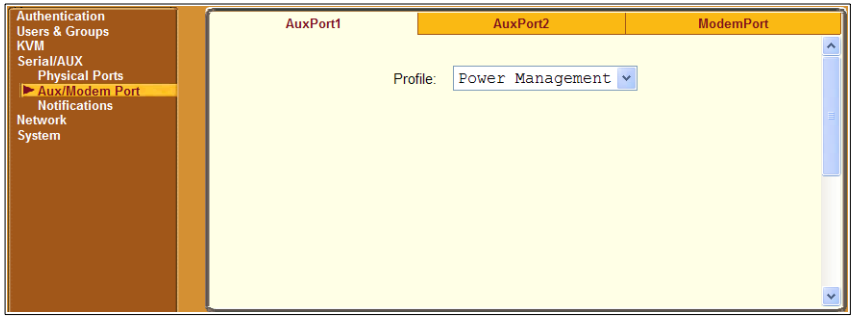


Figure 6-38: Web Manager Configuration>Serial/AUX>Aux/Modem Port Screen

An administrative user can use either the AuxPort1 and AuxPort2 screens to enable and to configure an auxiliary port if one of the following is connected to an AUX port:

- One or multiple daisy-chained AlterPath PM IPDUs
- An external modem

Power Management and AUX Ports

The following are important concepts for understanding the relationship between AUX ports, IPDU power management while connected, and serial and KVM ports.

- Both AUX ports can be connected to and configured to support either of the following:
  - An external modem for PPP connection
  - An AlterPath PM IPDU for power management
- For AUX port 2, certain restrictions apply to what kind of power management can be done.
  - If you plug a server that is connected to a KVM port into an IPDU connected to AUX2, no one can perform power management while connected to that server through the KVM port.

- AUX port 2 can be used for power management while connected only for devices connected to a serial port.

The following table shows the power management options for the two AUX ports.

Table 6-18: Power Management Options for AUX Ports

Port	Power Management Options	Types of devices
AUX 1	From the Web Manager Access>IPDU Power Management menu	Any server or other device connected to either a KVM or a serial port
	While connected to a serial or KVM port through the Web Manager or directly to a serial port through a console session.	Any server or other device connected to either a serial or KVM port
AUX 2	From the Web Manager Access>IPDU Power Management menu	Any server or other device connected to either a KVM or a serial port
	While connected to a serial port through the Web Manager or through a console session.	Any server or other device connected to a serial port

When either the AuxPort1 or AuxPort2 tabs are selected under Configuration>Serial/AUX>Aux/Modem Port in Expert mode, the screen shown in the following figure appears, if “Power Management” is selected on the “Profile” pull-down menu.

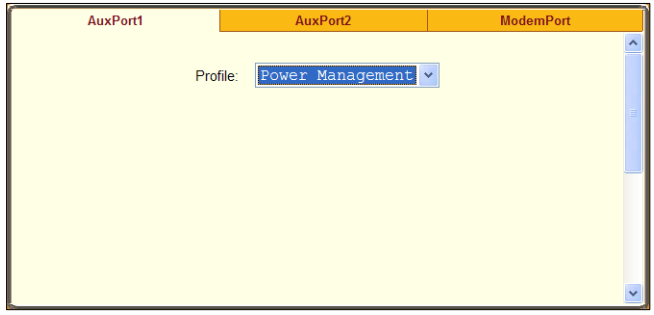


Figure 6-39: Web Manager Configuration>Serial/AUX>Aux/Modem Port>AuxPort1 and AuxPort2—Power Management

PPP and the AUX and Modem Ports

When configuring PPP connections to an external modem connected to an AUX port or to the modem port, an administrative user can use the AuxPort1 or AuxPort2 or ModemPort screens to change the default settings, if desired. The settings are shown in the following screen examples and in Table 6-19, “Fields for Configuring PPP on AuxPort or ModemPort Screens,” on page 261.

When you go to the screens for either AuxPort1 or AuxPort2 under Configuration>Aux/Modem Port in Expert mode, the screen in the following figure appears if “PPP” is selected on the “Profile” pull-down menu.

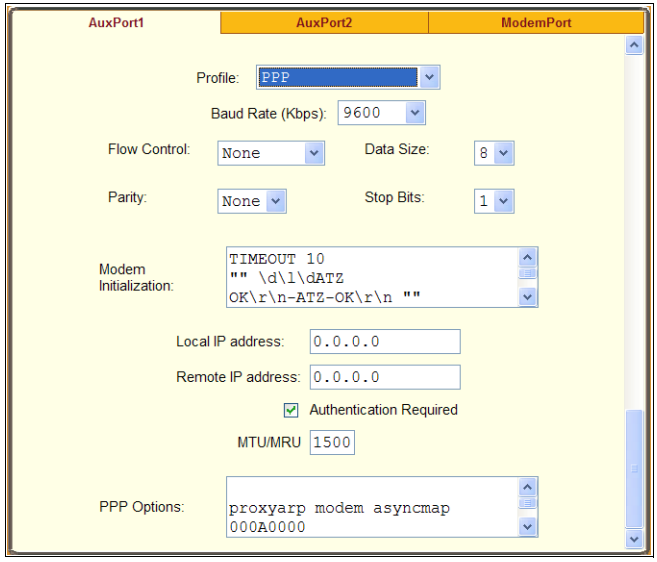


Figure 6-40: Web Manager Configuration>Serial/AUX>Aux/Modem>AuxPort1 and AuxPort2—PPP

When you go to Configuration>Serial/AUX>Aux/Modem Port>ModemPort in Expert mode, the screen shown in the following figure appears.

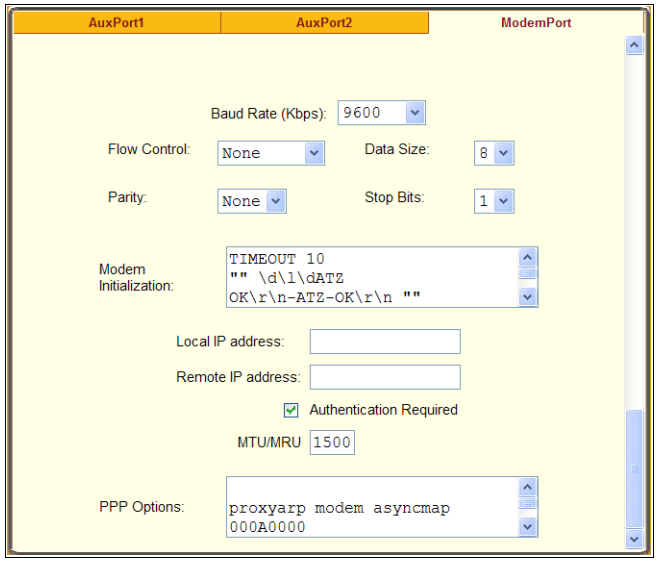


Figure 6-41: Web Manager Configuration>Serial/AUX>Aux/Modem>Modem Port Screen

The following table defines the information you need to specify when PPP is selected from the “Profile” pull-down menu on the AuxPort screens or the ModemPort screen.

Table 6-19: Fields for Configuring PPP on AuxPort or ModemPort Screens (Sheet 1 of 3)

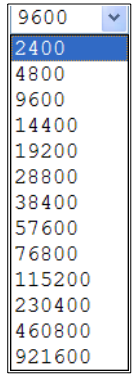
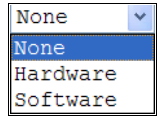
Field Name	Definition
Baud Rate (Kbps)	The baud rate of the modem. Default is 9600. 
Flow Control	The flow control used by the modem. Default is None. 
Data Size	The data size from 5 to 8.
Parity	“None,” “Odd,” or “Even.”
Stop Bits	The number of stop bits: “1” or “2.”

Table 6-19: Fields for Configuring PPP on AuxPort or ModemPort Screens (Sheet 2 of 3)

Field Name	Definition

Modem Initialization	The modem initialization string is used to configure the modem when it is turned on or when the communications software calls another modem. The default is:
	`TIMEOUT 10`
	`"" \d\l\dATZ`
	`OK\r\n-ATZ-OK\r\n ""`
	`TIMEOUT 10`
	`"" ATM0`
	`OK\r\n ""`
	`TIMEOUT 3600`
	`RING ""`
	`STATUS Incoming %p:I.HANDSHAKE`
	`"" ATA`
	`TIMEOUT 60`
	`CONNECT@ ""`
	`STATUS Connected %p:I.HANDSHAKE`
	If you need to change how the modem is initialized, see Table 6-20, "Commonly-Used Supported AT Commands," on page 263.

Local IP Address	The local IP address used by PPP to set up the session between the local and the remote modem. By default, the IP address of the OnSite is used. Use the default unless you have a specific reason to use another IP address.
Remote IP Address	The remote IP address used by PPP to set up the session between the local and the remote modem. By default, the IP address 10.0.0.1 is used. Use the default unless you have a specific reason to use another IP address.

Table 6-19: Fields for Configuring PPP on AuxPort or ModemPort Screens (Sheet 3 of 3)

Field Name	Definition
Authentication Required	Check the checkbox to require authentication.
MTU/MRU	The maximum transmission unit / maximum receive units for the PPP.

PPP Options	The default options are:
	`proxyarp modem asyncmap 000A0000`
	`noipx noccp login novj require-pap refuse-chap`
	`ms-dns 0.0.0.0`
	`plugin /usr/lib/libpsr.so`

AT Commands for Modem Initialization

In most cases, the default modem initialization commands are acceptable. For when changes are necessary, this section provides a brief introduction to the AT (*AT*tention code) commands that are used to control the modem's operation. The command format is AT*Xn*, where *X* is the command and *n* is the numeric value for the command. If the value is 0 (zero), it can be omitted from the command. For example, AT&W is the same as AT&W0. The following table defines the most-commonly-used commands: ATA, ATD, ATH, ATM, ATV, ATZ, AT&F, and AT&W.

Table 6-20: Commonly-Used Supported AT Commands (Sheet 1 of 4)

Command	Definition
AT	Attention Code.
	Precedes all command lines except A/, A:, and escape sequences.
A	Answer call before final ring.
A/	Repeat last command.

Table 6-20: Commonly-Used Supported AT Commands (Sheet 2 of 4)

Command	Definition
D*s*	Dial telephone number *s*, where *s* is the dial string modifier, which may be up to 40 characters long and include the 0–9, *, #, B, C, and D characters, and the L, P, T, V, W, S, comma (,), semicolon (;), !, @, ^, and $ dialstring modifiers. Dial string modifiers: L – Redial last number. (Must be placed immediately after ATD.) P – Pulse-dial following numbers in command. T – Tone-dial following numbers in command (default). V – Switch to speakerphone mode and dial the following number. Use ATH command to hang up. W – Wait for a new dial tone before continuing to dial. (X2, X4, X5, X6, or X7 must be selected.) , – Pause during dialing for time set in register S8. ; – Return to command mode after dialing. (Place at end of dial string.) ! – Hook flash. Causes the modem to go on-hook for one-half second, then off-hook again. @ – Wait for quiet answer. Causes modem to wait for a ringback, then 5 seconds of silence, before processing next part of command. If silence is not detected, the modem returns a NO ANSWER code. ^ – Disable data calling tone transmission. $ – Detect AT&T call card “bong” tone. The character should follow the phone number and precede the user’s call card number as in the following example: ATDT102880612785350$123456789.
DS=*y*	Dial stored telephone number. *y*=0-2 Dial a number previously stored in a directory number *y* by the &Z*y*=*x* command. Example: ATDS=2.

Table 6-20: Commonly-Used Supported AT Commands (Sheet 3 of 4)

Command	Definition
H*n*	Hook control. *n* = 0 or 1 Default: 0 H0 – Go on-hook (hang up). H1 – Go off-hook (make the phone line busy).
M*n*	Monitor speaker mode. *n* = 0, 1, 2, or 3 Default: 1 M0 – Speaker always off. M1 – Speaker on until carrier signal detected. M2 – Speaker always on when modem is off-hook. M3 – Speaker on until carrier is detected, except while dialing.
V*n*	Result code format. *n* = 0, 1, or 2 Default: 1 V0 – displays result codes as digits (terse response). V1 – Displays result codes as words (verbose response).
Z	Modem reset. Resets modem to profile saved by the last &W command.
&F	Load factory settings as active configuration.

Table 6-20: Commonly-Used Supported AT Commands (Sheet 4 of 4)

Command	Definition
&W*n*	Store current configuration. *n* = 0 or 1 Stores current modem settings in non-volatile memory and causes them to be loaded at power-on or following the ATZ command instead of the factory defaults. See also the &F command. &W1 Clears user default settings from non-volatile memory and causes the factory defaults to be loaded at power-on or following the ATZ command.

▼ To Configure an AUX Port for IPDU Power Management [Expert]

This procedure assumes an AlterPath PM intelligent power distribution unit (IPDU) is connected to one of the AUX ports.

1. Go to Configuration >Serial/AUX>Aux/Modem Port in Expert mode.
2. Select either the AuxPort1 or AuxPort2 tab, as appropriate.
3. Make sure the checkbox next to “Enable Port” is checked.
4. Make sure the “Power Management” option is selected from the “Profile” menu.
5. Click “apply changes.”

▼ To Configure an AUX Port for PPP [Expert]

This procedure assumes an external modem is connected to the selected AUX port.

1. Go to Configuration >Serial/AUX>Aux/Modem Port in Expert mode.
2. Select either the AuxPort1 or AuxPort2 tab, as appropriate.
3. Make sure the checkbox next to “Enable Port” is checked.
4. From the “Profile:” pull-down menu, select PPP or Login.

   Additional fields appear on the screen.

5. Accept or change the following values to match the modem's values:
   - "Baud Rate"
   - "Flow Control"
   - "Data Size:"
   - "Parity"
   - "Stop Bits"
6. Accept or make any changes desired to the modem initialization commands in the "Modem Initialization:" text area.
7. For PPP, do the following steps.
   a. Enter an IP address in the "Local IP" field.
   b. In the "Remote IP" field, specify the IP address to assign to the other end of the PPP connection.
   c. Check or leave unchecked the checkbox next to "Authentication Required."
   d. Accept or change the number in the "MTU/MRU" field.
   e. Accept or make any changes desired to the PPP options in the "PPP Options" text area.
8. Click "apply changes."

▼ *To Configure the Internal Modem [Expert]*

1. Go to Configuration >Serial/AUX>Aux/Modem Port in Expert mode.
2. Select the ModemPort tab.
3. Make sure the checkbox next to "Enable Port" is checked.
4. Accept or change the following values to match the modem's values:
   - "Baud Rate"
   - "Flow Control"
   - "Data Size:"
   - "Parity"
   - "Stop Bits"

5. Accept or make any changes desired to the modem initialization commands in the “Modem Initialization:” text area.
6. For PPP, do the following steps.
   a. Enter an IP address in the “Local IP” field.
   b. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection.
   c. Check or leave unchecked the checkbox next to “Authentication Required.”
   d. Accept or change the number in the “MTU/MRU” field.
   e. Accept or make any changes desired to the PPP options in the “PPP Options” text area.
7. Click “apply changes.”

Configuration>Serial/AUX>Notifications

Selecting Configuration>Serial/AUX>Notifications in Expert mode brings up a screen like the one shown in the following figure.

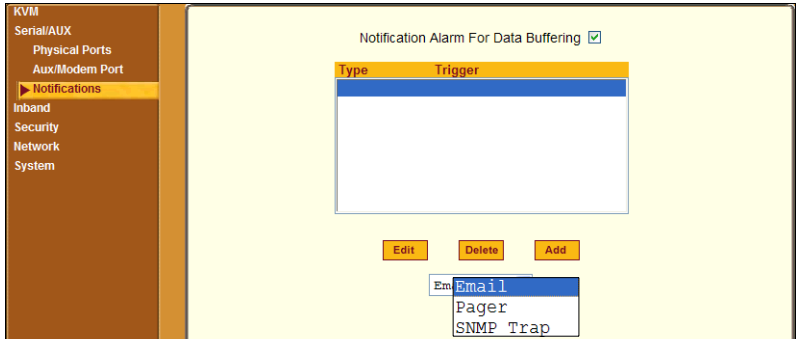


Figure 6-42: Web Manager Configuration>Serial>Notifications Screen

An administrative user can use this screen to enable notifications about system crashes or other events of interest that occur on the device that is connected to the serial port. Data buffering must be enabled. The administrative user an configure notifications to be sent either by email, pager, or SNMP trap.

Caution! Alarms are not generated unless the checkbox is checked next to "Notification Alarm for Data Buffering."

Clicking the Add button or selecting a previously-specified event and clicking the Edit button brings up a "Notifications Entry" dialog box that allows you to define trigger actions and specify how to handle them. Different fields appear on the dialog boxes depending on whether Email, Pager, and SNMP trap notifications have been chosen. Figure 6-43 shows the dialog box for email notifications.

Note: Until an alarm trigger is specified, the pull-down menu on the "Notifications Entry" screen is empty. A new trigger gets listed in the menu after it is created.

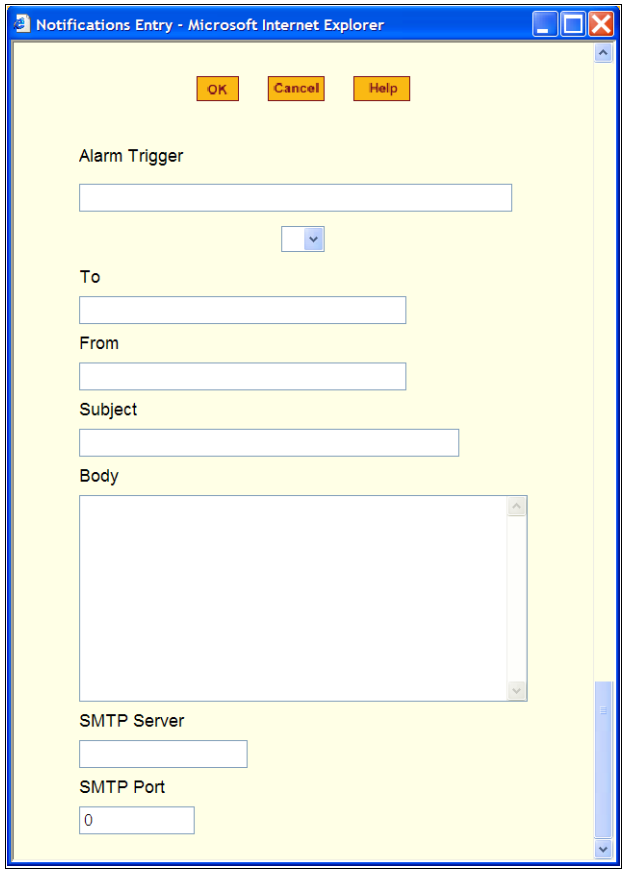


Figure 6-43: Web Manager Configuration>Serial/AUX>Notifications—Email Example

See “Notifications, Alarms, and Data Buffering” on page 28 for the supported syntax for alarm triggers.

▼ *To Choose a Method for Sending Notifications for Serial Port Data Buffering Events [Expert]*

1. Go to Configuration>Serial/AUX>Notifications in Expert mode.

   The Notifications screen appears.

2. Click the checkbox next to “Notification Alarm for Data Buffering.”

3. Select “Email,” “Pager,” or “SNMP trap” from the pull-down menu.
4. To create a new entry for an event to trigger an alarm or notification, click the Add button.
5. To edit a previously-configured trigger, click the Edit button.
6. Go to one of the following procedures.
   - “"To Configure a Trigger for Email Notification for Serial Ports [Expert]
   - “To Configure a Trigger for Pager Notification for Serial Ports [Expert]” on page 272
   - “To Configure a Trigger for SNMP Trap Notification for Serial Ports Expert]” on page 272

▼ *To Configure a Trigger for Email Notification for Serial Ports [Expert]*

1. Go to Configuration>Serial/AUX>Notifications in Expert mode, select “Email” from the pull-down menu; optionally, configure an alarm to sound when the trigger action occurs; and click either Add or Edit.

   If needed, see “To Choose a Method for Sending Notifications for Serial Port Data Buffering [Expert]” on page 217.
2. Specify the function you want to trigger a notification in the “Alarm Trigger” field using the required syntax.
3. Enter the recipient for notification email in the “To” field.

   Enter the *username* only in this field. The email is sent to *username@server*, where *server* is the value entered in Step 7.
4. Enter an email address identifying the OnSite in the “From” field.
5. Enter the subject in the “Subject” field.
6. Enter an explanatory text message in the “Body” field.
7. Enter the SMTP server’s IP address or DNS name in the “SMTP Server” field.
8. Enter the SMTP port number in the “SMTP Port” field.

▼ To Configure a Trigger for Pager Notification for Serial Ports [Expert]

1. Go to Configuration>Serial/AUX>Notifications in Expert mode, select Pager from the pull-down menu; optionally, configure an alarm to sound when the trigger action occurs; and choose “Pager” from the pull-down menu, and click either Add or Edit.

   If needed, see “To Choose a Method for Sending Notifications for Serial Port Data Buffering [Expert]” on page 217.

   The “Notifications Entry” dialog box appears.

2. Specify the function you want to trigger a notification in the “Alarm Trigger” field using the required syntax.
3. Select “Pager” from the pull-down menu.
4. Enter the pager number in the “Pager Number” field.
5. Enter the text that describes the event in the “Text” field.
6. Enter the Short Message Services (SMS) user name, the SMS server’s IP address or name, and the SMS port number in the “SMS User Name,” “SMS Server,” and “SMS Port” fields.
7. Click “OK.”

▼ To Configure a Trigger for SNMP Trap Notification for Serial Ports Expert]

1. Go to Configuration>Serial/AUX>Notifications in Expert mode, select “SNMP Trap” from the pull-down menu; optionally, configure an alarm to sound when the trigger action occurs; and click either Add or Edit.

   If needed, see “To Choose a Method for Sending Notifications for Serial Port Data Buffering [Expert]” on page 217.

2. Specify the function you want to trigger a notification in the “Alarm Trigger” field using the required syntax.
3. Enter the number in the “OID Type Value” field.
4. Configure the appropriate trap number from the “Trap Number” pull-down menu.

The choices are “Cold Start,” “Warm Start,” “Link Down,” “Link up,” “Authentication Failure,” “EGP neighbor loss,” or “Enterprise specific.”

5. Enter a community in the “Community” field.
6. Enter the IP address or name of a SNMP Server.
7. Enter a message in the “Body” text area.
8. Click “OK.”

Configuration>Inband

Selecting Configuration>Inband in Expert mode brings up a screen like the one shown in the following figure.

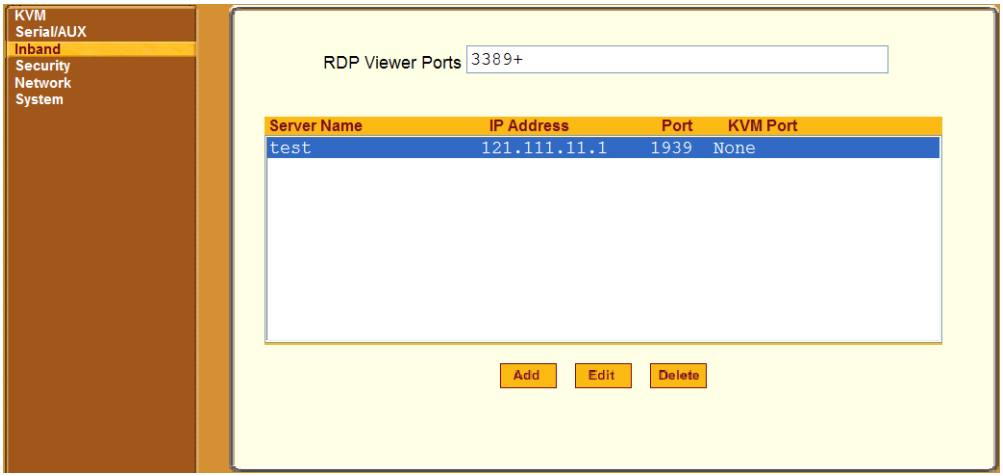


Figure 6-44: Web Manager Configuration>Inband Screen

Administrative users can use the Inband screen to configure one of the following two types of access to Windows servers that have RDP enabled:

- Inband-only access to servers that are not connected to KVM ports
- AdaptiveKVM access to servers that are connected to KVM ports (inband access is provided as long as the server is fully operational and accepting RDP requests, with automatic fallback to KVM over IP access if inband access fails)

See “Inband” on page 43 for more details about the technology.

Clicking the “Add” or “Edit” buttons brings up a dialog with the fields shown in the following figure.

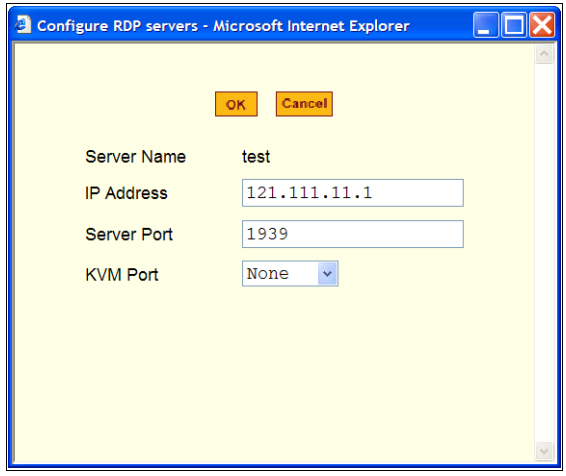


Figure 6-45: Web Manager Configuration>Inband Edit Screen

The following table describes the values to enter on the Add and Edit screens.

Table 6-21: Inband Configuration Values

Field	Description
Server Name	A unique name for the server. **Note:** The server name cannot be modified. The only way to change a name is to delete the server’s entry and add it again.
IP Address	The IP address of the server
Server Port	If the port differs from the default, supply the desired port name here. **Note:** The default server port for servers with RDP enabled is 3389.
KVM Port	To enable AdaptiveKVM when the RDP server is connected to a KVM port, enter the KVM port’s name or alias.

Configuration>Security

Selecting Configuration>Security in Expert mode brings up three options in left menu as shown in the following figure.

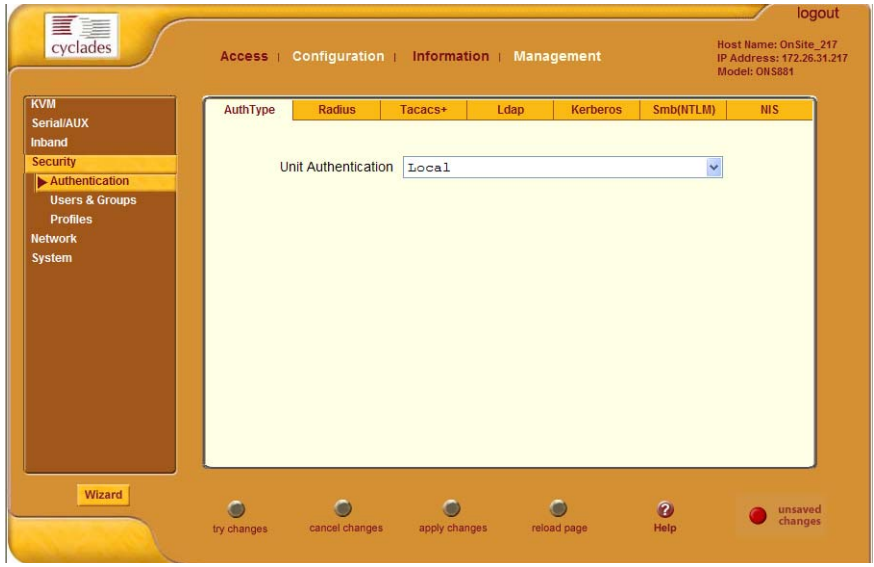


Figure 6-46: Web Manager Configuration>Security Menu Options

Administrative users can use the Security screens to configure network-related features, as described in the following sections:

Configuration>Security>Authentication

Selecting Configuration>Security>Authentication in Expert mode brings up the seven tabs shown in the following figure.

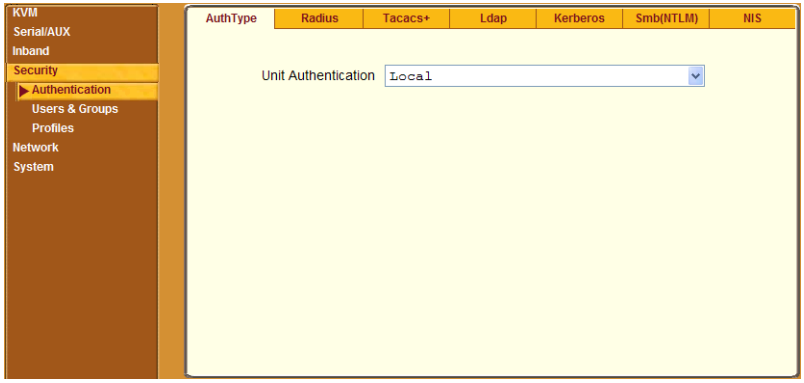


Figure 6-47: Web Manager Authentication Tab Options

An administrative user can use the Authentication screens for the two following related tasks:

- Select a method for authenticating logins to the OnSite *only.*

  See “Configuring Authentication for OnSite Logins” on page 277.

- Identify all authentication servers for authentication during logins to the OnSite or to ports

  See “Configuring Authentication Servers” on page 278.

For selecting an authentication method for logins to devices connected to KVM and serial ports, the screens are under Configuration>KVM and Configuration>Serial. See the following sections, if desired, for how to select an authentication method for ports:

See “Authentication” on page 26 of Chapter 1 for an overview of authentication on the OnSite, if needed.

Configuring Authentication for OnSite Logins

The default authentication method for the AlterPath OnSite is Local. An administrative user can either accept the default or select another authentication method from the pull-down menu on the AuthType screen.

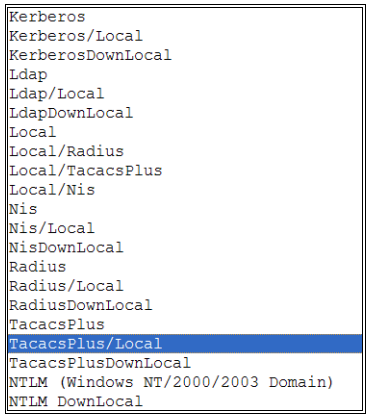


Figure 6-48: Authentication “AuthType” Options

Any authentication method chosen for the OnSite is used for authentication of any users attempting to log into the OnSite through `telnet`, `ssh`, or the Web Manager.

▼ To Configure an OnSite Login Authentication Method [Expert]

See “Authentication” on page 158, if needed, for background information.

1. Go to Configuration>Authentication in Expert mode.

   The “AuthType” screen displays, as shown in the following figure.

2. To specify an authentication method for logins to the OnSite, select a method from the “Unit Authentication” pull-down menu.

3. Click “apply changes.”

4. Make sure that an authentication server is specified for the selected authentication type.

   See “Configuring Authentication Servers for Logins to the OnSite and Connected Devices.”

Configuring Authentication Servers

The administrator fills out the appropriate screen to set up an authentication server for every authentication method to be used by the OnSite and by any of its ports: Kerberos, LDAP, NIS, NTLM/SMB (ports only), RADIUS, TACACS+.

The following table lists the procedures that apply to each authentication method.

Table 6-22: Tasks for Setting up Authentication Servers for Each Authentication Method

Method	Variations	Procedures
Kerberos	Kerberos, Local/Kerberos, Kerberos/Local, or Kerberos/DownLocal	"To Configure a Kerberos Authentication Server [Expert]" on page 279
LDAP	LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal	"To Configure an LDAP Authentication Server [Expert]" on page 281
NIS	NIS, Local/NIS, NIS/Local, or NIS/DownLocal	"To Configure a NIS Authentication Server [Expert]" on page 285
NTLM (Windows NT/2000/2003 Domain)	NTLM (Windows NT/2000/2003 Domain), or NTLM/DownLocal	"To Configure an SMB(NTLM) Authentication Server [Expert]" on page 283
RADIUS	RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal	"To Configure a RADIUS Authentication Server [Expert]" on page 285
TACACS+	TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal	"To Configure a TACACS+ Authentication Server [Expert]" on page 286

▼ *To Configure a Kerberos Authentication Server [Expert]*

Perform this procedure to configure a Kerberos authentication server when the OnSite or any of its ports is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local, or KerberosDownLocal).

Before starting this procedure, find out the following information from the Kerberos server's administrator:

- Realm name and KDC address
- Host name and IP address for the Kerberos server

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If Kerberos authentication is specified for the OnSite, accounts for all users who need to log into the OnSite to administer connected devices.
- If Kerberos authentication is specified for KVM or serial ports, accounts for users who need administrative access to connected devices

1. Make sure an entry for the OnSite and the Kerberos server exist in the OnSite's `/etc/hosts` file.

   a. Go to Configuration>Network>Host Table in Expert mode.

      The "Host Table" screen appears.

   b. Add an entry for OnSite if none exists and an entry for the Kerberos server.

      i. Click "Add."

      The "New/Modify Host" dialog appears.

      ii. Enter the address in the "IP Address" field.

      iii. Enter the name in the "Name" field.

      iv. If desired, enter an optional alias in the "Alias" field.

2. Make sure that timezone and time and date settings are synchronized on the OnSite and on the Kerberos server.

Note: Kerberos authentication depends on time synchronization. Time and date synchronization is most easily achieved by setting both the OnSite and the Kerberos server to use the same NTP server.

a. To specify an NTP server, follow the procedure under "To Configure Time and Date [Expert]" on page 350.

b. To manually set the time and date on the OnSite, follow "To Configure the Time Zone [Expert]" on page 349.

c. Work with the authentication server's administrator to synchronize the time and date between the OnSite and the server.

3. If the OnSite is not located in the PST time zone, set the timezone on the OnSite.

a. Make a console connection to the OnSite and log in as root,

```
AlterPath Onsite login: root
Password: ********
```

The root prompt appears.

```
[root@onsite root]#
```

b. Enter **set_timezone**.

A list of timezones appears followed by a prompt asking you to enter a number of a timezone.

```
[root@onsite root]# set_timezone
Please choose the time zone where this machine is located.
0) GMT
1) 1h West GMT
2)10h West GMT
...
26) 9h East GMT
Enter your option:
```

c. Enter the number of the timezone where the OnSite is located.

```
Enter your option: 10
```

d. Logout from the console session and close the terminal.

4. In the Web Manager Expert mode, go to Configuration>Authentication> Kerberos.

The Kerberos screen displays as shown in the following figure.

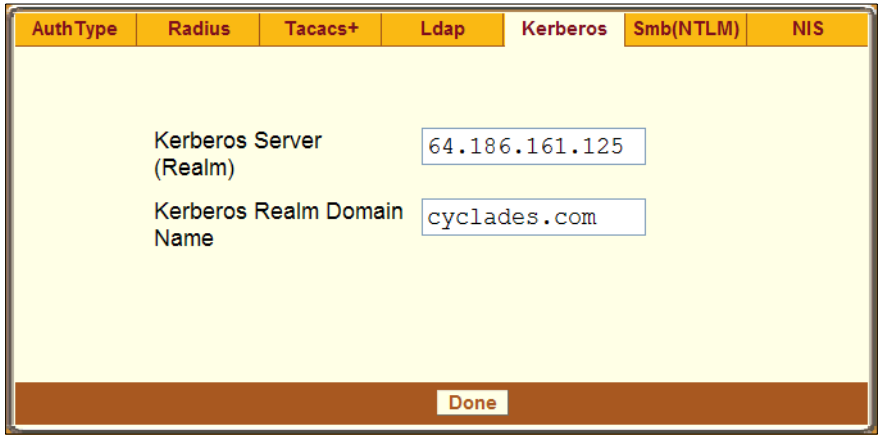


Figure 6-49: Web Manager Kerberos Authentication Server Screen

5. Fill in the screen according to your local setup of the Kerberos server.

6. Click “Done.”

7. Click “apply changes.”

▼ *To Configure an LDAP Authentication Server [Expert]*

Perform this procedure to configure an LDAP authentication server when the OnSite or any of its ports is configured to use the LDAP authentication method or any of its variations (LDAP, Local/LDAP, LDAP/Local, or LDAP/ DownLocal).

Before starting this procedure, find out the following information from the LDAP server's administrator:

- The distinguished name of the search base
- The LDAP domain name
- Whether to use secure LDAP
- The authentication server's IP address

An administrative user can enter information in the following two fields, but an entry is not required:

- The LDAP password
- The LDAP user name

Work with the LDAP server's administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If LDAP authentication is specified for the OnSite, accounts for all users who need to log into the OnSite to administer connected devices.
- One or more groups listing all the users
- If LDAP authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.

Make sure to configure a group or groups on the OnSite with the same names and members as the group or groups on the LDAP authentication server. (See "To Add a Group [Expert]" on page 295.)

1. Go to Configuration>Authentication>LDAP in Expert mode.

The "LDAP" screen displays with "LDAP Server" and "LDAP Search Base" fields filled in from the current values in the `/etc/ldap.conf` file.

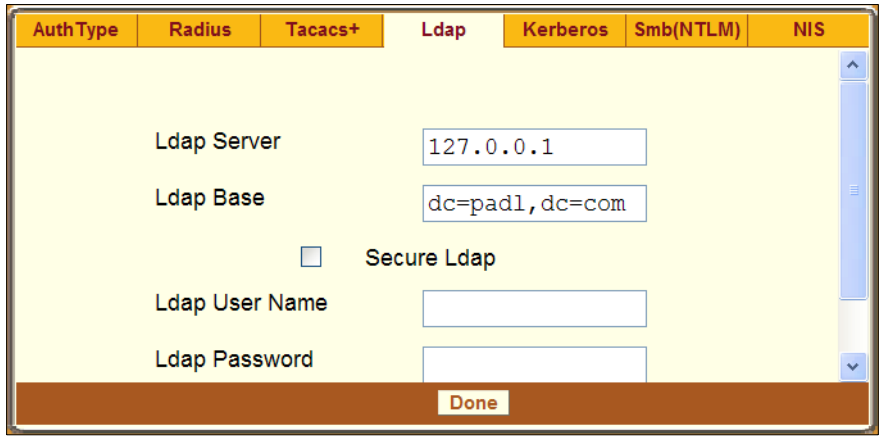


Figure 6-50: Web Manager LDAP Authentication Server Screen

2. Supply the IP address of the LDAP server in the “LDAP Server” field.
3. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the “LDAP” Base field, change the definition.

   The default distinguished name is “dc,” as in `dc=value,dc=value`. If the distinguished name on the LDAP server is “o,” then replace `dc` in the base field with `o`, as in `o=value,o=value.`
4. Replace the default base name with the name of your LDAP domain.

   For example, for the LDAP domain name cyclades.com, the correct entry is: `dc=cyclades,dc=com`.
5. Click “Done.”
6. Click “apply changes.”

   The changes are stored in `/etc/ldap.conf` on the OnSite.

▼ *To Configure an SMB(NTLM) Authentication Server [Expert]*

Perform this procedure to configure an SMB(NTLM) authentication server if any of the ports is configured to use the NTLM (Windows NT/2000/2003 Domain) authentication method or NTLM/Downlocal local fallback option.

Work with the NTLM server's administrator to ensure that following types of accounts are set up on the NTLM server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- One or more groups listing all the users
- If NTLM authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.

Make sure to configure a group or groups on the OnSite with the same names and members as the group or groups on the NTLM authentication server. (See "To Add a Group [Expert]" on page 295.)

1. Go to Configuration>Authentication>SMB(NTLM) in Expert mode.

   The SMB(NTLM) screen displays as shown in the following figure.

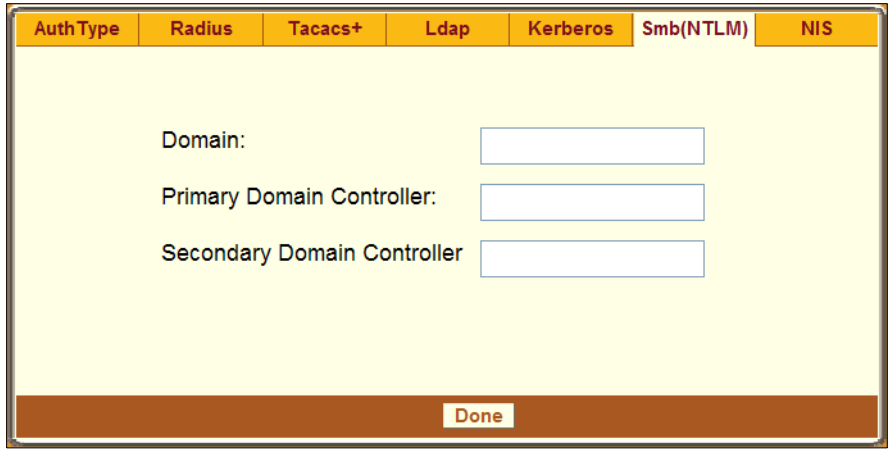


Figure 6-51: Web Manager SMB(NTLM) Authentication Server Screen

2. Fill in the screen according to your configuration of the SMB server.
3. Click "Done."
4. Click "apply changes."

▼ To Configure a NIS Authentication Server [Expert]

Perform this procedure to identify the authentication server when the OnSite or any of its ports is configured to use the NIS authentication method or any of its variations (Local/NIS, NIS/Local, or NIS/DownLocal).

1. Go to Configuration>Authentication>NIS in Expert mode.

   The NIS screen displays as shown in the following figure.

Figure 6-52: Web Manager NIS Authentication Server Screen

2. Fill in the screen according to your configuration of the NIS server.
3. Click “Done.”
4. Click “apply changes.”

▼ To Configure a RADIUS Authentication Server [Expert]

Perform this procedure to identify the authentication server when the OnSite or any of its ports is configured to use the RADIUS authentication method or any of its variations (Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal).

1. Go to Configuration>Authentication>RADIUS in Expert mode.

   The RADIUS screen displays as shown in the following figure.

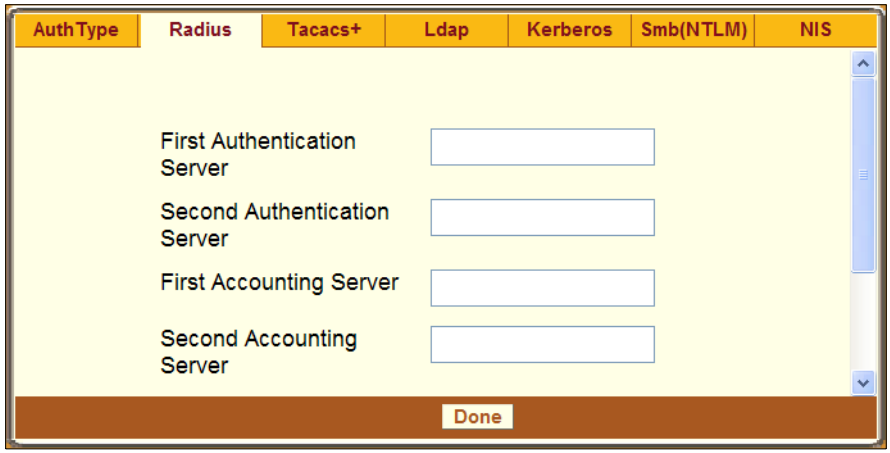


Figure 6-53: Web Manager Radius Authentication Server Screen

2. Fill in the screen according to your local setup of the RADIUS server or servers.
3. Click “Done.”
4. Click “apply changes.”

   The changes are stored in `/etc/raddb/server` on the OnSite.

▼ *To Configure a TACACS+ Authentication Server [Expert]*

Perform this procedure to configure a TACACS+ authentication server when the OnSite or any of its ports is configured to use the TACACS+ authentication method or any of its local fallback options (Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal).

Work with the TACACS+ server’s administrator to ensure that following types of accounts are set up on the TACACS+ server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for “admin.”
- If TACACS+ authentication is specified for the OnSite, accounts for all users who need to perform administrative tasks with the users assigned to a group called “admin.”

See “Configuring Groups for TACACS+” on page 512 for how the groups are configured on the TACACS+ server.

- One or more groups listing all the users
- If TACACS+ authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.

Make sure to configure a group or groups on the OnSite with the same names and members as the group or groups on the TACACS+ authentication server. (See “To Add a Group [Expert]” on page 295.)

1. Go to Configuration>Authentication>TACACS+ in Expert mode.

   The TACACS+ screen appears.

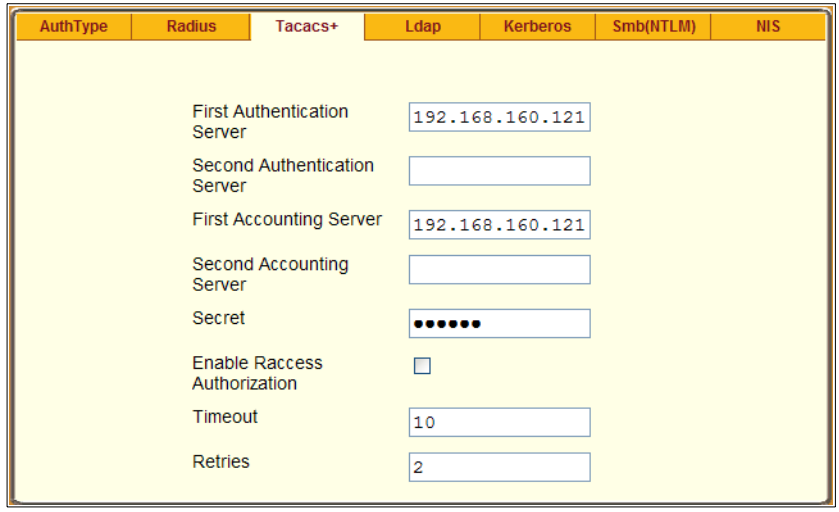


Figure 6-54: Web Manager TACACS Authentication Server Screen

2. Fill in the screen according to your local setup of the TACACS+ server or servers.

Note: “Enable Raccess Authorization” must be checked if groups are configured as in “To Add a Group [Expert]” on page 295.

---

3. Click “Done.”
4. Click “apply changes.”

The changes are stored in `/etc/tacplus.conf` on the OnSite.

Configuration>Security>Users & Groups

Selecting Configuration>Security>Users & Groups in Expert mode brings up a screen like the one shown in the following figure.

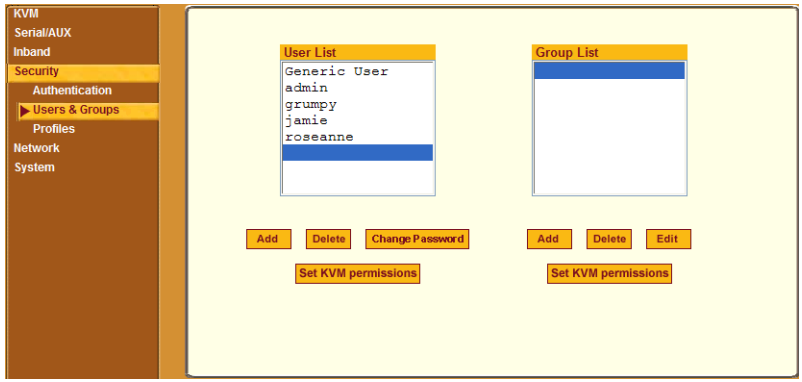


Figure 6-55: Web Manager Configuration>Security>Users & Groups Screen

An administrative user can use the Users & Groups screen to do the following:

- Add or delete users
- Assign or change user passwords
- Add or delete groups
- Add users to a group
- Delete users from a group
- Set the KVM port access permissions of the Generic User
- Set unique KVM port access permissions for a individual user or group of users:
  - Assign default KVM access permissions to users or groups
  - Set specific access permissions for users and groups for a selected KVM port or ports.

The Generic User defines the KVM port access permissions for all users except administrative and root users. Any new regular user account automatically inherits the KVM port access permissions configured for the Generic User unless you take the additional step of configuring the user's

KVM port access permissions differently as described under “Setting KVM Port Permissions” on page 291. For more background about the hierarchy of KVM port permissions, see “Understanding KVM Port Permissions” on page 32 and “KVM Port Permissions Hierarchy” on page 34.

Adding a User

If the “Add” button is clicked on the Configuration>Security>Users & Groups screen, the following dialog box appears.

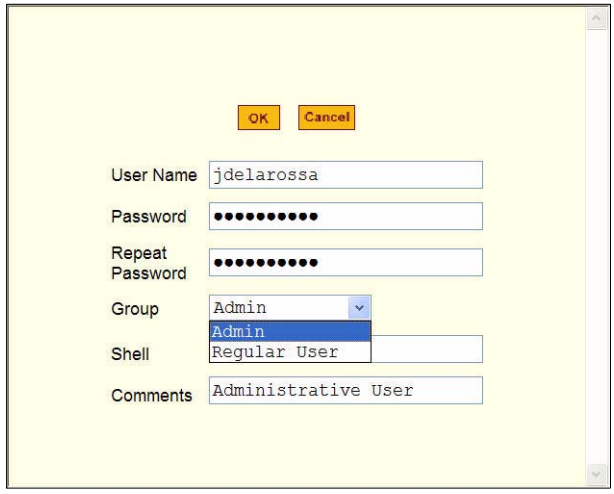


Figure 6-56: Configuration>Security>Users & Groups “Add Dialog Box”

The following table defines the fields.

Table 6-23: Add User Dialog: Field Names and Definitions

Field Name	Definition
User Name	Name of the user to be added.
Password	The password associated with the user name.
Group	On the Group pull-down menu, select “Regular User [Default]” or “Admin.” **Note:** To configure a user to be able to perform all administrative functions, select the “Admin” group. See “Types of Users” on page 18 for more details.

Table 6-23: Add User Dialog: Field Names and Definitions (Continued)

Field Name	Definition
Shell	Optional. The default shell when the user makes a `ssh` or `telnet` connection with the switch. Choices are: `sh` [Default] or `bash`.
Comments	Optional notes about the user's role or configuration.

Adding a Group

If the "Add" button is clicked the Configuration>Security>Users & Groups screen under the Group list, the "Add Group" dialog box shown in the following figure appears.

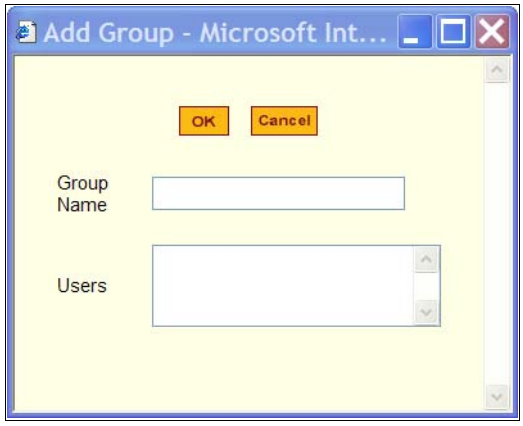


Figure 6-57: Configuration>Security>Users & Groups "Add Group" Dialog Box

A new group is defined by entering a group name and a comma-separated list of users.

Setting KVM Port Permissions

If a user or group name is selected from the list of users and groups and the "Set KVM Permissions" button is clicked on the Configuration>Security>Users & Groups screen, a "KVM Access List" screen appears like the one in the following figure.

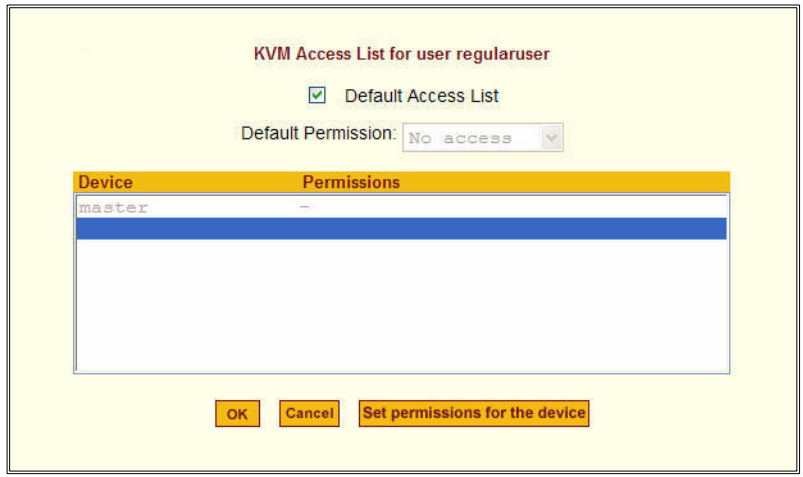


Figure 6-58: Users & Groups Configuration "KVM Access List" Screen

When the "Default Access List" checkbox is checked, the selected user or group has the same permissions that are assigned to the Generic User.

If the checkbox is unchecked, KVM port access permissions can be configured for a user or group to be different from the Generic User by doing the following:

- Choosing a user-specific "Default Permission"
- Specifying explicit permissions for specific ports

If the "Default Access List" checkbox on the KVM Access List dialog box is deselected, the "Default Permission" pull-down menu becomes active with the options: "No access," "Read only," "Read/Write," "Full access," as shown in the following figure.

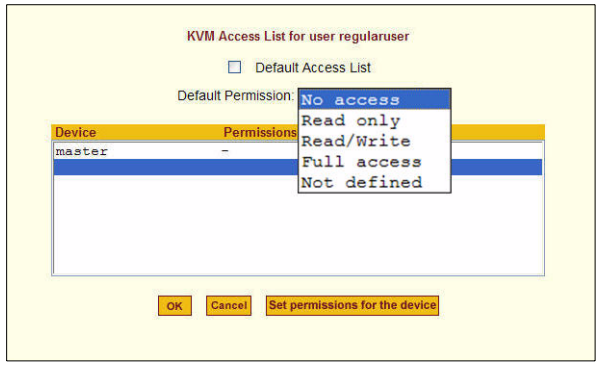


Figure 6-59: KVM Access List “Default Permissions” Menu Options

For an example of how the “Default Permissions” work, if the Generic User’s default permission is “No access” and you remove the check from the checkbox next to “Default Access List” for a user named jamesi, then jamesi is no longer restricted by the permissions of the Generic User. If you then assign to jamesi a default permission of “Full access,” jamesi can then read write and do power management while connected to any KVM port.

If the “Default Access List” option is deselected, the “master” device is selected from the Device/Permissions list and the “Set permissions for the device” button is checked, a dialog box appears like the one shown in following figure.

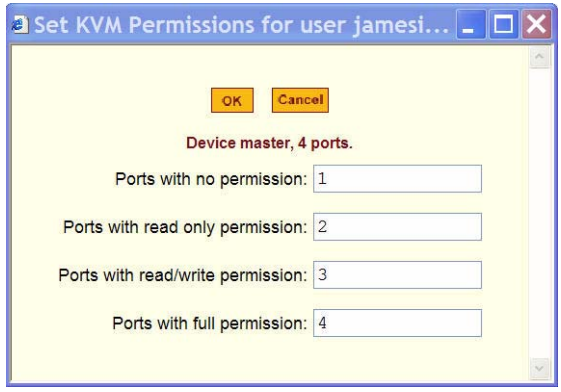


Figure 6-60: “Set KVM Permissions” Ports Permissions Dialog Box

Separate lists of ports can be specified with any of the following permissions for any user or group:

- Ports with no permission
- Ports with read only permission
- Ports with read/write permission
- Ports with full permission (read, write, and power management)

The permissions display next to the Device name in the Permissions column, as shown in the following figure.

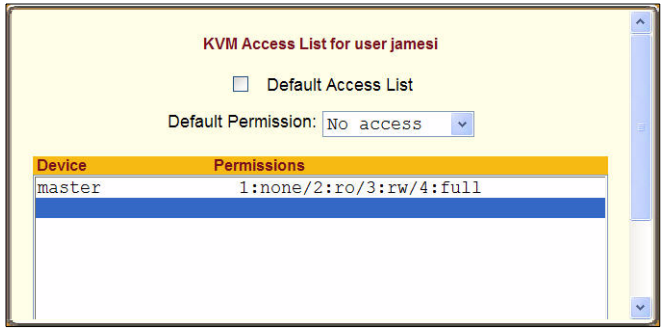


Figure 6-61: Set KVM Permissions “KVM Access List” Example

The following figure illustrates how the settings in the previous figure affect access to ports. When an individual or member of a group with the access permissions shown in the previous screen logs into the Web Manager, the list of KVM ports displayed does not include port 1 because it was configured with no access (shown as “none”).

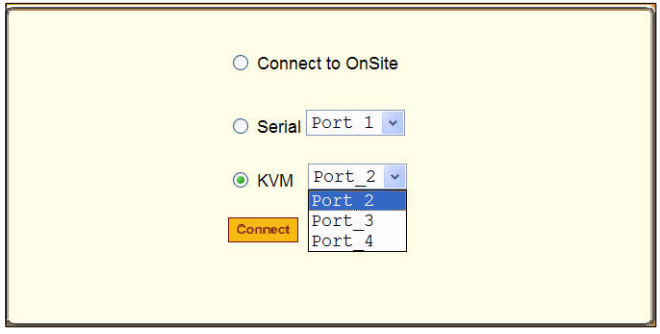


Figure 6-62: KVM Port Access Restriction Example

To continue the example, because of the KVM permission settings, jamesi can connect to KVM port 2 with Read Only access, he can connect to ports 3 with Read Write access, and he can connect to port 4 with Read/Write/Power Management access.

▼ To Add a User [Expert]

1. Go to Configuration>Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.

2. Click “Add.”

   The “Add User” dialog box displays.

3. Enter the name in the “User Name” field.
4. Enter the password in the “Password” and “Repeat Password” fields.
5. Assign a group from the “Group” pull-down menu.
6. Optional: Select a shell from the “Shell” pull-down menu.
7. Optional: Enter information, as desired, about the user’s role or responsibilities.
8. Click OK.
9. Click “apply changes.”

▼ To Delete a User or Group [Expert]

1. Go to Configuration>Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.

2. Select the name of a user or group to delete.
3. Click “Delete.”
4. Click “apply changes.”

▼ To Change a User’s Password [Expert]

1. Go to Configuration>Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.

2. Select the name of the user whose password you want to change.
3. Click “Change Password.”

   The Change User Password” dialog box displays.
4. Enter the new password and enter it gaining the “New Password” and “Repeat New Password” fields.
5. Click OK.
6. Click “apply changes.”

▼ *To Add a Group [Expert]*

1. Go to Configuration>Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.
2. Under the list of groups, click “Add.”

   The “Add Group” dialog box displays.
3. Enter the name for the new group in the “Group Name” field.
4. Enter one user name or multiple comma-separated user names in the “Users” field.
5. Click OK.
6. Click “apply changes.”

▼ *To Modify a Group [Expert]*

1. Go to Configuration>Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.
2. Select the name of a group to modify.
3. Click “Edit.”

   The “Edit Group” screen displays.
4. Add or delete users from the group as desired.
5. Click OK.
6. Click “apply changes.”

▼ To Select Users and Groups for Assigning KVM Port Access [Expert]

Perform this procedure to select users to access servers connected to KVM ports.

1. Go to Configuration >Security>Users & Groups in Expert mode.

   The Users & Groups screen displays.

2. To set KVM port access for a regular user, select the name of the user from User List.

3. To set KVM port access permissions for a group, select the name of the group from the Group List.

4. Click the “Set KVM Permissions” button.

   The “KVM Access list for *username*” or “*groupname* “dialog box appears.

▼ To Assign KVM Ports to a User or Group [Expert]

Perform this procedure when you want to specify the types of access a user or group of users can have to computers that are connected to the OnSite’s KVM ports.

1. Go to Configuration>Security>Users & Groups in Expert mode and select a user or group.

2. To assign to the selected user or group the same permissions assigned to the Generic User, make sure the “Default Access List” checkbox is checked and click OK.

3. To assign KVM port access permissions for the selected user or group, uncheck the “Default Access List” checkbox.

4. Select the desired default access option from the “Default Permission:” pull-down menu.

5. To configure access to individual ports or groups of ports, select the master device from the “Device/Permissions” list.

6. Click the “Set permissions for the device” button.

The “Set KVM Permissions for the device” dialog box displays as shown in the following figure. (The example shows the dialog box when the “master” device is selected.)

In the fields for each desired category, type either port aliases or numbers, separating them either by commas or dashes.

7. Click OK.

   The newly-set permissions display next to the Device name in the Permissions column.

8. Click OK.

9. Click “apply changes.”

Configuration>Security>Profiles

Selecting Configuration>Security>Profiles in Expert mode brings up a screen like the one shown the following figure.

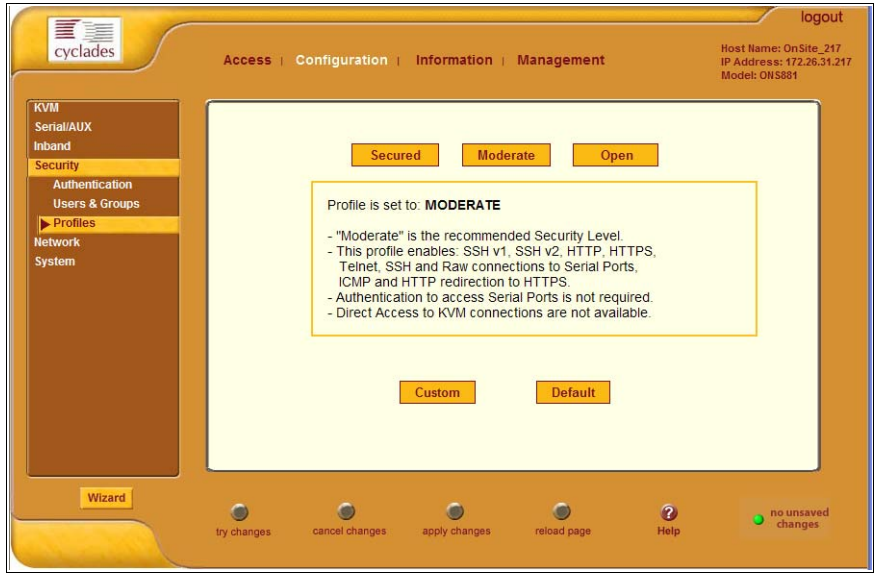


Figure 6-63: Web Manager Configuration>Security>Profiles Screen

The procedures for configuring a security profile are identical in both Wizard and Expert modes. See “Step 1: Security Profile [Wizard]” on page 163 for details.

Configuration>Network

Selecting Configuration>Network in Expert mode brings up nine options in left menu as shown in the following figure.

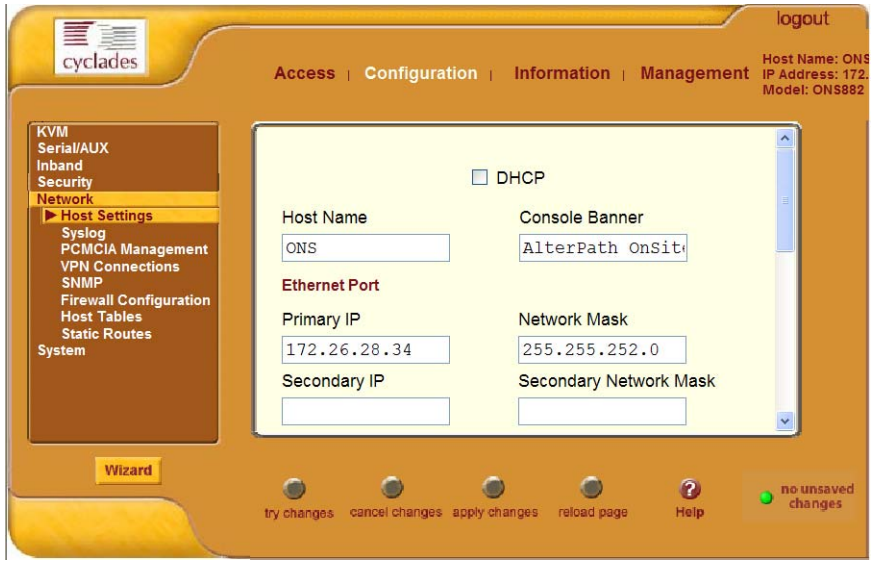


Figure 6-64: Web Manager Configuration>Network Options

An administrative user can use the Network screens to configure network-related features, as described in the following sections:

- “Configuration>Network>Host Settings” on page 299
- “Configuration>Network>Syslog” on page 303
- “Configuration>Network>PCMCIA Management” on page 305
- “Configuration>Network>VPN Connections” on page 320
- “Configuration>Network>SNMP” on page 323
- “Configuration>Network>Firewall Configuration” on page 327
- “Configuration>Network>Host Tables” on page 342
- “Configuration>Network>Static Routes” on page 343

Configuration>Network>Host Settings

When Configuration>Network>Host Settings is selected in Expert mode, the following screen appears.

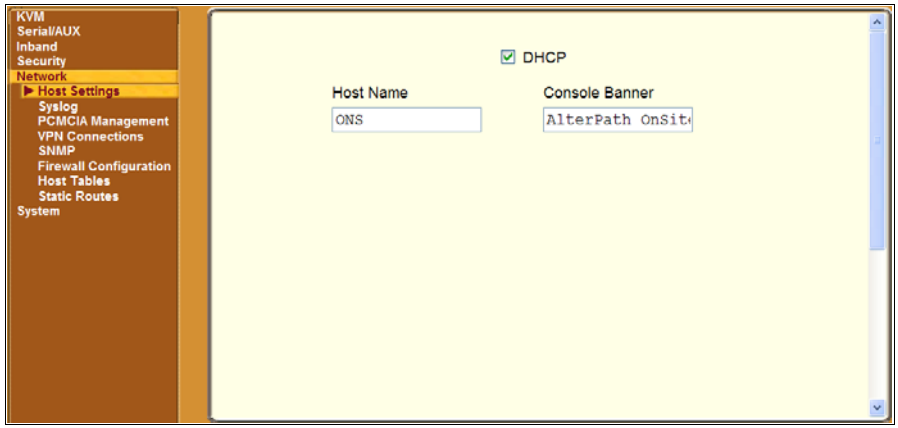


Figure 6-65: Web Manager Configuration>Network>Host Settings Screen

An administrative user can use the Host Settings screen to configure a name and IP address for the OnSite and configure basic networking parameters.

If the “DHCP” checkbox is not checked, then other options appear on the screen as shown in the following example.

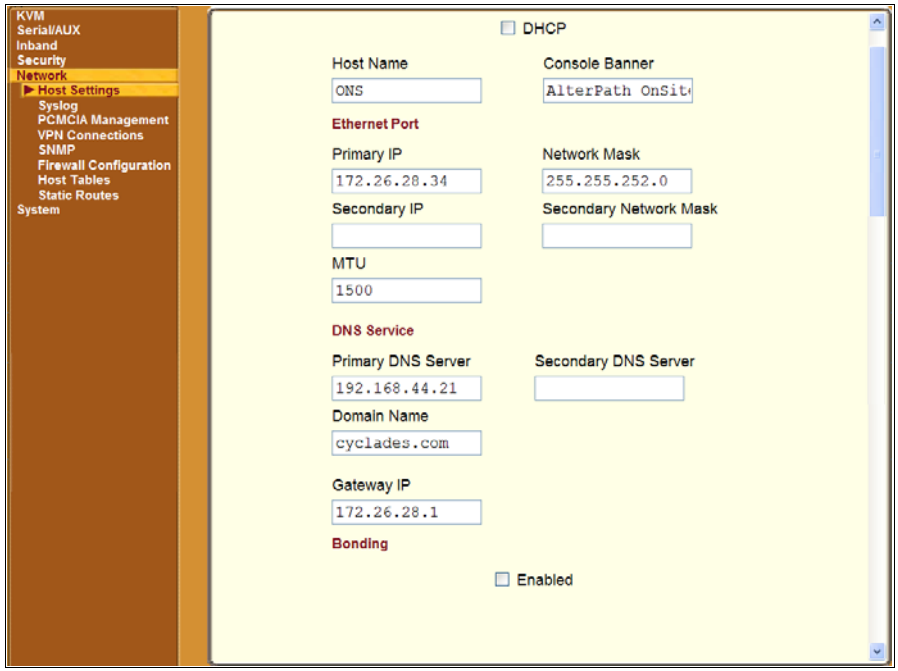


Figure 6-66: Web Manager Configuration>Network>Host Settings Screen—No DHCP

The following table describes the fields on the Host Settings form.

Table 6-24: Host Settings Form Fields (Sheet 1 of 2)

Filed Name	Field Definition
Host Name	The fully qualified DNS name identifying the OnSite on the network.
Console Banner	A text string designed to appear on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection.
Primary IP	IP address of the OnSite.
Secondary IP	An optional secondary IP address for the OnSite unit.
Network Mask	The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for a subnet.

Table 6-24: Host Settings Form Fields (Sheet 2 of 2)

Filed Name	Field Definition
Secondary Network Mask	Optional.
MTU	Maximum Transmission Unit used by the TCP protocol.
DNS Server	Address of the Domain Name Server.
Secondary DNS Server	Address of the backup Domain Name Server.
Domain Name	The name that identifies the domain, for example, domainname.com.
Gateway IP	The IP address to the gateway on the subnet.
Bonding	Enables redundancy for the Ethernet devices using the standard Ethernet interface as the primary mode of access and a PCMCIA card as a secondary mode of access. If bonding is enabled, the following values should be set. **Miimon:** The interval in which the active interface is checked to see if it is still communicating (in milliseconds). **Updelay**: The time that the system will wait to make the primary interface active after it has been detected as up (in milliseconds).

▼ *To Configure Hosts [Expert]*

1. Go to Configuration>Network>Host Settings in Expert mode.

   The Host Settings screen appears:

2. By default, DHCP is enabled. To disable DHCP, click the checkbox to remove the check mark.

   Additional fields appear.

3. Under Ethernet Port, complete or edit the following fields, as necessary.

a. Enter the name assigned to the IP address of the OnSite in the “Host Name” field.

b. Enter or change the console banner in the “Console Banner” field.

   The console banner appears on the console when the user logs into and exits from a port as a way to verify or identify the particular port connection

c. Enter the IP address of the OnSite in the “Primary IP” field.

d. Enter the netmask in the “Network Mask” field.

e. Enter an optional secondary IP address in the “Secondary IP” field.

f. Specify the netmask of the secondary IP in the “Secondary Network Mask” field.

g. Specify the desired maximum transmission unit in the “Maximum Transmission Unit” field.

4. Under “DNS Service” specify or change the following information, if desired.

   a. Enter the address of the domain name server in the “Primary DNS Server” field.

   b. If there is a backup DNS server, enter the address of the secondary DNS in the “Primary DNS Server” field

   c. Enter the domain in the “Domain Name” field.

   d. Enter the IP address of the gateway in the “Gateway IP” field.

5. To enable Ethernet failover (bonding), do the following steps.

   a. Click the “Enabled” checkbox under “Bonding.”

      “Miimon” and “Updelay” fields appear.

   b. If desired, change the value in the “miimon” field.

      The default is 100.

   c. If desired, change the value in the “Updelay” field.

      The default is 200.

6. Click “apply changes.”

Configuration>Network>Syslog

When Configuration>Network>Syslog is selected in Expert mode, the screen shown in the following figure appears.

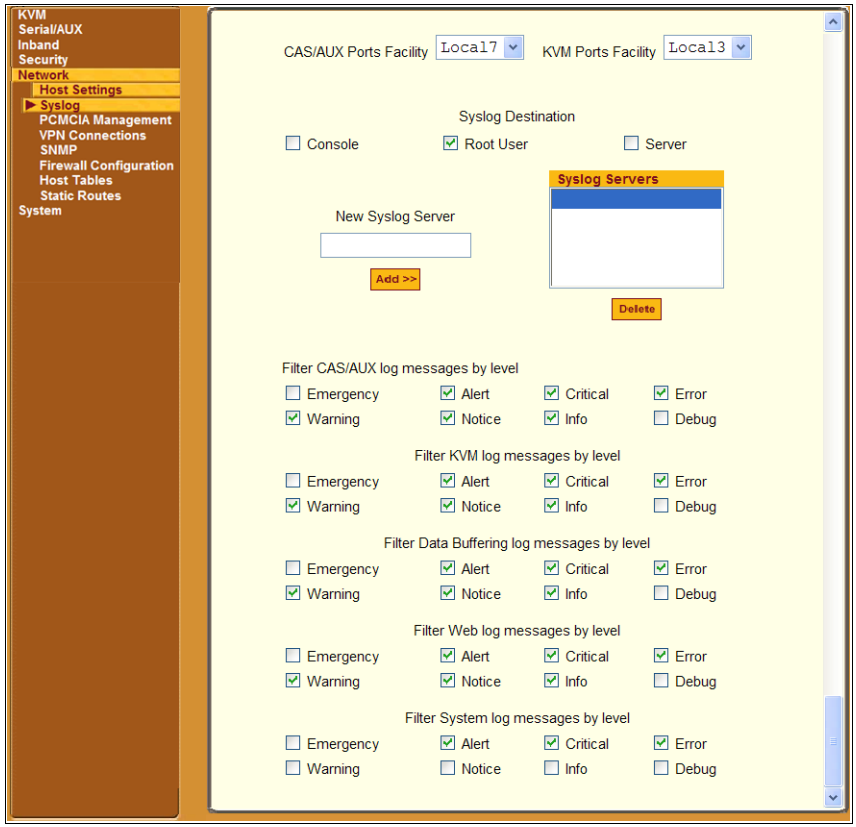


Figure 6-67: Web Manager Configuration>Network>Syslog Screen

An administrative user can use the Syslog screen to configure how the OnSite handles syslog messages. The Syslog screen allows you to do the following:

- Specify one or more syslog servers to receive syslog messages related to ports.
- Specify rules for filtering messages.

The top of the screen is used to tell the OnSite where to send syslog messages:

- One facility number can be specified for messages from serial ports and AUX ports and another facility number for messages from KVM ports.

  See “Facility Numbers for Syslog Messages” on page 28 for details.

  Obtain the facility numbers to use from the syslog server’s administrator. See ““To Add a Syslog Server [Wizard]” on page 183 for how a syslog server is configured for the OnSite. The same server or different syslog servers and the same or duplicate facility numbers can be specified according to your site’s configuration.
- Syslog messages can be sent to the console port (for logging the messages even if no user is logged in); to all sessions where the root user is logged in, or to one or more syslog servers.
- Entries for syslog servers can be added or deleted.

The bottom of the screen has checkboxes for specifying which types of messages are forwarded based on the following criteria:

- Their severity level: “Emergency,” “Alert,” “Critical,” “Error,” “Warning,” “Notice,” “Info,” “Debug”
- Their category “CAS/AUX log;” “KVM log;” “Data Buffering log;” “Web log;” or “System log.”

▼ *To Configure Syslogging and Message Filtering [Expert]*

1. Go to Configuration>Network>Syslog in Expert mode.

   The Syslog screen displays.
2. Select a destination for the Syslog messages by clicking the checkbox next to one or more of the options: “Console,” “Root User,” or “Server.”
3. Add a syslog server to the Syslog Servers list, by entering its IP address in the “New Syslog Server” field, and clicking the “Add>>” button.
4. Select a facility number for messages generated by serial or AUX ports by selecting the number from the “CAS/AUX Ports Facility” pull-down menu.
5. Select a facility number for messages generated by KVM ports by selecting the number from the “KVM Ports Facility” pull-down menu.

6. Click “apply changes.”

Configuration>Network>PCMCIA Management

When Configuration>Network>PCMCIA Management is selected in Expert mode, the following screen appears.

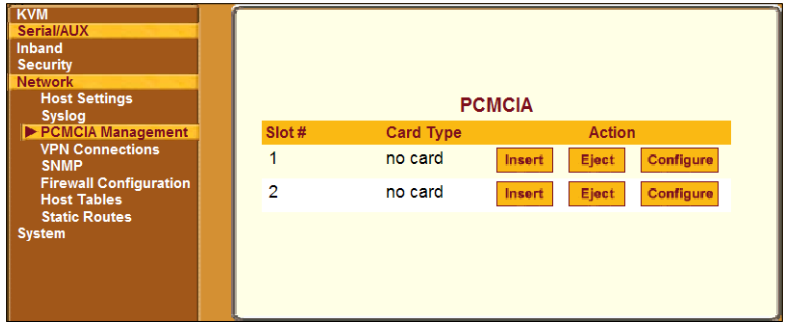


Figure 6-68: Web Manager Configuration>Network>PCMCIA Management Screen

An administrative user can use the PCMCIA management screen to configure the following types of PCMCIA cards:

- Modem
- ISDN
- GSM
- Ethernet (10/100BaseT and Fibre)
- Compact Flash / Hard Disk
- Wireless
- CDMA

The menu is shown in the following figure:

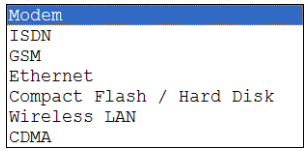


Figure 6-69: Web Manager Configuration>Network> PCMCIA Management Menu

While configuring a PCMCIA card, you must inserted a card in one of the PCMCIA slots on the front of the OnSite.

For configuring call back, you need to have the phone number of the remote modem calling in.

▼ *To Begin Configuring a PCMCIA Card [Expert]*

1. Insert a PCMCIA card into one of the slots on the front of the OnSite.
2. Go to Configuration>Network>PCMCIA Management in Expert mode.

   The PCMCIA Management page appears.
3. Click the “Insert” button on the line for the slot in which you installed the PCMCIA card.

   The card type appears under the “Card Type” column.
4. Click the Configure button.

   The “Slot” dialog box appears.
5. Select the desired PCMCIA card type to configure from the pull-down menu.
6. Go to the appropriate procedure.

To Configure a Modem PCMCIA Card [Expert]	Page 308
To Configure an ISDN PCMCIA Card [Expert]	Page 310
To Configure a GSM PCMCIA Card [Expert]	Page 312
To Configure an Ethernet PCMCIA Card [Expert]	Page 313
To Configure a Compact Flash or Hard Disk PCMCIA Card [Expert]	Page 315
To Configure a Wireless LAN PCMCIA Card [Expert]	Page 316

Configuring a Modem PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network to enable remote users to dial into the OnSite through an installed modem PCMCIA card. When the administrative user selects Modem from the pull-down menu, the dialog box shown in the following figure appears.

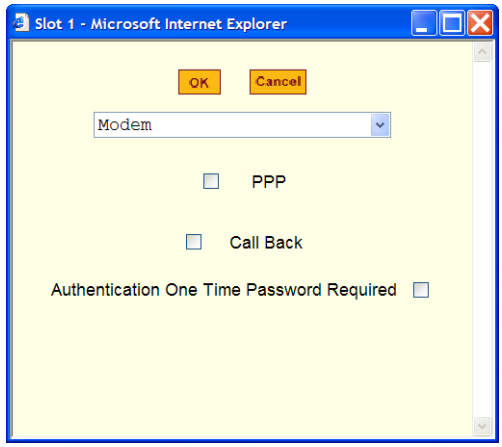


Figure 6-70: Modem PCMCIA Card Configuration Dialog Box

As shown in Figure 6-70, the following appear on the dialog:

- "PPP" checkbox
- "Call Back" checkbox
- "Authentication One Time Password Required" checkbox

If the "PPP" checkbox is checked, additional fields for a local and remote IP address appear, and if the "Call Back" checkbox is checked, a "Phone Number" field appears, as shown in the following figure.

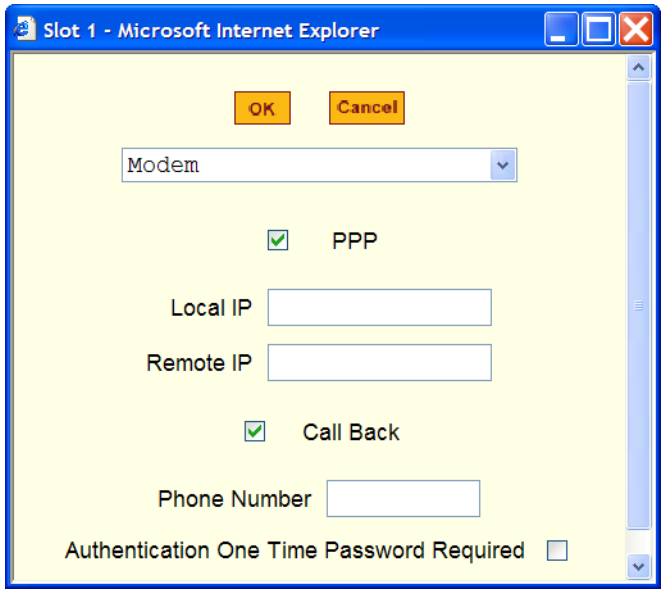


Figure 6-71: Modem PCMCIA Card Configuration Dialog Box—PPP and Call Back Checkboxes Checked

▼ *To Configure a Modem PCMCIA Card [Expert]*

1. Install the modem card and select “Modem” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

2. To enable PPP, do the following steps:

   a. Check the PPP checkbox.

   b. Enter an IP address in the “Local IP” field, if desired.

      By default, the IP address of the OnSite is used. Only change the IP address if you have a specific reason to do so.

   c. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

3. To enable call back, do the following:
   a. Check the “Call Back” check box.
   b. Enter a number to use to call back the modem.
4. To configure authentication using OTP passwords, check the “Authentication One Time Password Required” checkbox.

Note: OTP authentication works only if an OnSite administrator has performed the prerequisite configuration described in “One Time Password Authentication on the OnSite” on page 18.

---

5. Click OK.
6. Click “apply changes.”

Configuring an ISDN PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network in Expert mode to enable users to connect to the OnSite through an ISDN PCMCIA card. When you select ISDN from the pull-down menu, the dialog box shown in the following figure appears.

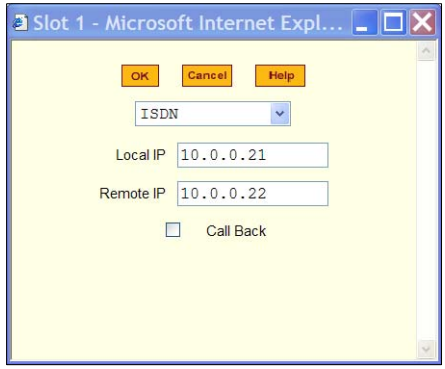


Figure 6-72: ISDN PCMCIA Card Configuration Dialog Box

When the “Call Back” checkbox is checked, the Phone Number field appears as shown in the following figure.

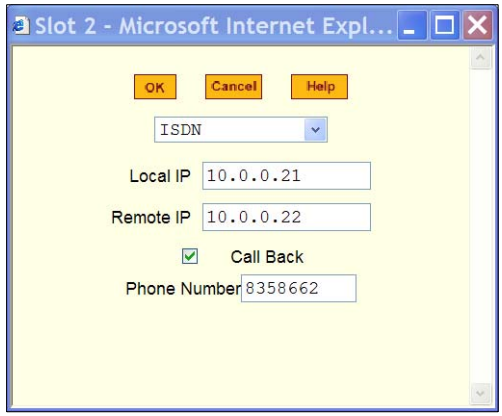


Figure 6-73: ISDN PCMCIA Card Configuration Dialog Box—Call Back

▼ *To Configure an ISDN PCMCIA Card [Expert]*

1. Install the ISDN card and select “ISDN” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed. The “Local IP” and “Remote IP” fields and the “Call Back” check box appear on the Slot dialog box.

2. Enter an IP address in the “Local IP” field, if desired.

   By default, the IP address of the OnSite is used. Only change the IP address if you have a specific reason to do so.

3. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

   By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

4. To enable call back, do the following:

   a. Check the “Call Back” check box.

      The “Phone Number” field appears on the Slot dialog box.

   b. Enter a number for the OnSite to use to call back the remote modem.

5. Click OK.

6. Click “apply changes.”

Configuring a GSM PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network in Expert mode to enable a remote user to call into the OnSite through an installed and configured GSM PCMCIA card. When you select GSM from the pull-down menu, the dialog box shown in the following figure appears.

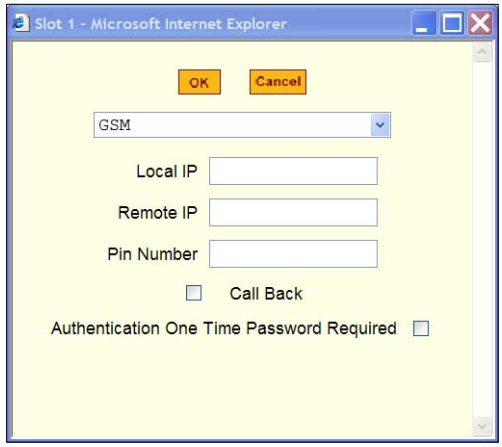


Figure 6-74: GSM PCMCIA Card Configuration Dialog Box

As shown in Figure 6-74, the following appear on the GSM configuration dialog:

- “Local IP” field
- “Remote IP” field
- “Pin Number” field
- “Call Back” checkbox
- “Authentication One Time Password Required” checkbox

When the “Call Back” checkbox is checked, the “Phone Number” field appears as shown in the following figure.

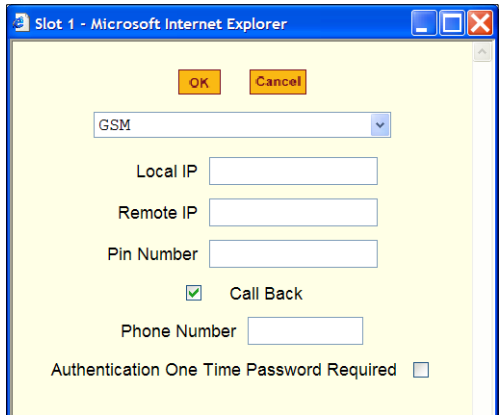


Figure 6-75: GSM PCMCIA Card Configuration Dialog Box—Call Back

▼ *To Configure a GSM PCMCIA Card [Expert]*

1. Install the GSM card and select “GSM” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

   The “Local IP,” “Remote IP,” and “Pin Number” fields and the “Call Back” check box appear on the Slot dialog box.

2. Enter an IP address in the “Local IP” field, if desired.

   By default, the IP address of the OnSite is used. Only change the IP address if you have a specific reason to do so.

3. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

   By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

4. Enter a personal identification number known to the owner of the GSM card in the “PIN Number” field.

5. To enable call back, do the following:

   a. Check the “Call Back” check box.

      The “Phone Number” field appears on the Slot dialog box.

b. Enter a number for the OnSite to use to call back the GSM phone.

6. To configure authentication using OTP passwords, check the "Authentication One Time Password Required" checkbox.

Note: OTP authentication works only if an OnSite administrator has performed the prerequisite configuration described in "One Time Password Authentication on the OnSite" on page 18.

---

7. Click OK.

8. Click "apply changes."

Configuring an Ethernet PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network in Expert mode to configure an Ethernet PCMCIA card. When you select Ethernet from the pull-down menu, the dialog box shown in the following figure appears.

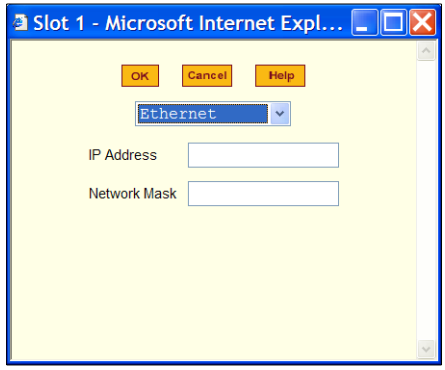


Figure 6-76: Ethernet PCMCIA Card Configuration Dialog Box

▼ *To Configure an Ethernet PCMCIA Card [Expert]*

Follow this procedure to configure either 10/100BaseT or Fibre PCMCIA cards.

1. Install the Ethernet card and select "Ethernet" from the pull-down menu on the PCMCIA Management screen.

See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

The “IP Address” and “Network Mask” fields appear on the Slot dialog box.

2. In the “IP address” field, enter the IP address to assign to the Ethernet port.
3. In the “Network Mask” field, enter the netmask to assign to the subnet.
4. Click OK.
5. Click “apply changes.

Configuring a Compact Flash PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network in Expert mode to configure a PCMCIA Compact Flash card. When you select Compact Flash from the pull-down menu, the dialog box shown in the following figure appears.

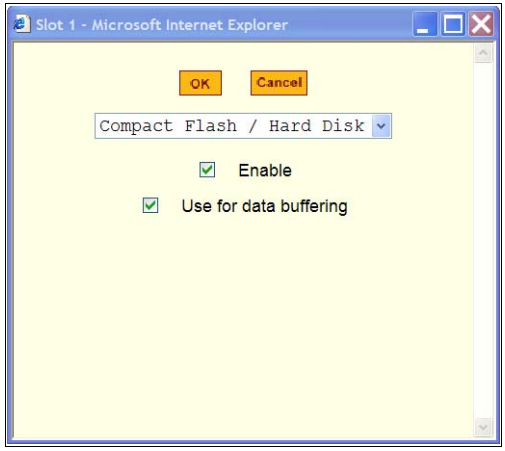


Figure 6-77: Compact Flash PCMCIA Card Configuration Dialog Box

▼ *To Configure a Compact Flash or Hard Disk PCMCIA Card [Expert]*

1. Install the compact flash card or IDE card and select “Compact Flash / Hard Disk” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

   The “Enable” and the “Use for data buffering” checkboxes appear on the Slot dialog box.

2. Click the “Enable” checkbox.
3. If desired, check the “Use for data buffering” checkbox.
4. Click OK.
5. Click “apply changes.”

Configuring a Wireless LAN PCMCIA Card

An administrative user can use the PCMCIA Management screen under Configure>Network in Expert mode to configure a Wireless LAN PCMCIA card. When you select “Wireless LAN” from the pull-down menu, the dialog box shown in the following figure appears.

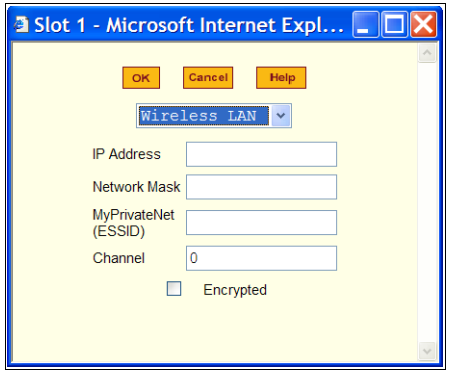


Figure 6-78: PCMCIA Wireless LAN Card Configuration Dialog Box

▼ To Configure a Wireless LAN PCMCIA Card [Expert]

1. Install the wireless LAN card and select “Wireless LAN” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

   The “IP Address,” “Network Mask,” “MyPrivateNet (ESSID),” and Channel fields appear on the Slot dialog box.
2. In the “IP address” field, enter an IP address.
3. In the “Network Mask” field, enter the netmask for the subnet.
4. In the “MyPrivateNet (ESSID)” field, enter the SSID for communicating with others in your network.
5. In the “Channel” field, enter a channel number.
6. Click the “Enable” checkbox.
7. Click OK.
8. Click “apply changes.”

Configuring a CDMA PCMCIA Card

The administrative user can use the PCMCIA Management screen under Configure>Network to enable a remote user to dial into the OnSite through an installed and configured CDMA PCMCIA card. When you select CDMA from the pull-down menu, the dialog shown in the following figure appears.

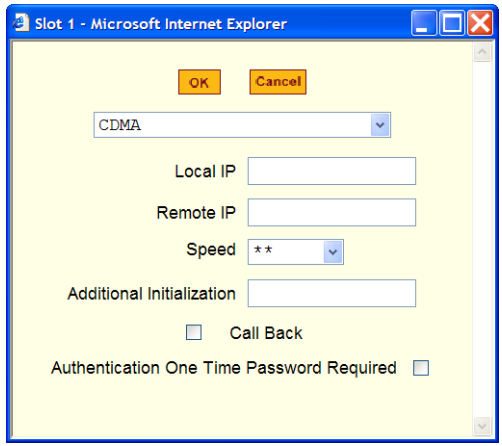


Figure 6-79: CDMA PCMCIA Card Configuration Dialog

As shown in Figure 6-79, the following appear on the CDMA configuration dialog:

- “Local IP” field
- “Remote IP” field
- “Speed” pull-down menu
- “Additional Initialization” field
- “Call Back” checkbox
- “Authentication One Time Password Required” checkbox

When the “Call Back” checkbox is checked, the Phone Number field appears as shown in the following figure.

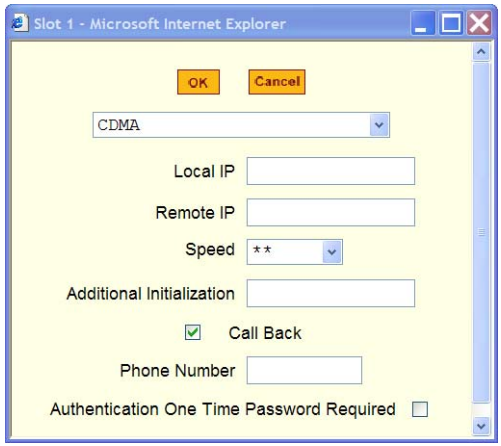


Figure 6-80: CDMA PCMCIA Card Configuration Dialog Box—Call Back

▼ *To Configure a CDMA PCMCIA Card [Expert]*

1. Install the CDMA card and select “CDMA” from the pull-down menu on the PCMCIA Management screen.

   See “To Begin Configuring a PCMCIA Card [Expert]” on page 306, if needed.

2. Enter an IP address in the “Local IP” field, if desired.

   By default, the IP address of the OnSite is used. Only change the IP address if you have a specific reason to do so.

3. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

   By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

4. Select a speed from the “Speed” pull-down menu.

5. To enable call back, do the following:

   a. Check the “Call Back” check box.

   b. Enter a number for the OnSite to use to call back the CDMA phone in the “Phone Number” field.

6. To configure authentication using OTP passwords, check the "Authentication One Time Password Required" checkbox.

Note: OTP authentication works only if an OnSite administrator has performed the perquisites configuration described in "One Time Password Authentication on the OnSite" on page 18.

---

7. Click OK.
8. Click "apply changes."

Ejecting a PCMCIA Card

Use the "Eject" button on the PCMCIA management screen to eject any PCMCIA card before physically ejecting it. Any other method can cause a kernel panic.

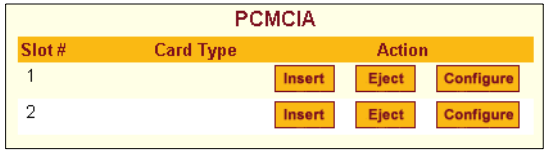
▼ *To Eject a PCMCIA Card From the Card Slot*

1. Go to Configuration>Network>PCMCIA Management.

   The PCMCIA Management page appears.

2. Click the Eject button adjacent to the card you want to remove.

   The card type clears under the Card Type column.



3. Click "apply changes."
4. Physically remove the card from the PCMCIA slot on the front of the OnSite.

Configuration>Network>VPN Connections

When Configuration>Network>VPN Connections is selected in Expert mode, a screen like the one shown in the following figure appears.

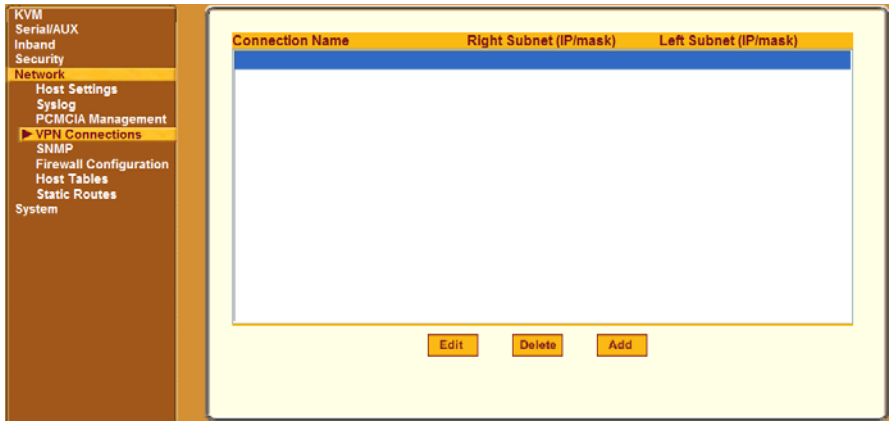


Figure 6-81: Web Manager Configuration>Network>VPN Connections Screen

An administrative user can use the screen to add a VPN connection or edit one that is already in the list. See “VPN on the OnSite” on page 54 for related background information.

When the “Edit” or “Add” buttons are clicked, a “New/Modify Connection” screen appears, as shown in the following figure. The screen displays different fields depending on whether “RSA Public Keys” or “Shared Secret” are selected.

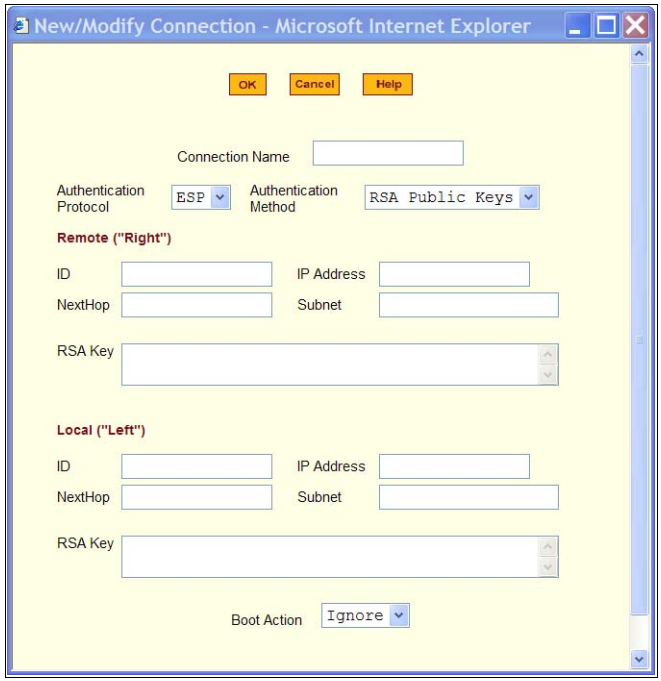


Figure 6-82: VPN “New/Modify Connection” Dialog Box

The OnSite is referred to as the Local or “Left” host, and the remote gateway is referred to as the Remote or “Right” host. If left and right are not directly connected, then you must also specify a NextHop IP address. The next hop for the left host is the IP address of the router to which the OnSite sends packets to get them delivered to the right host. The next hop for the right host is the IP address of the router to which the remote host or gateway running IPsec sends packets when delivering them to the left host. Also, because the OnSite can have multiple Ethernet connections and IP addresses, you need to enter the appropriate IP address and hostname in the “ID” and IP Address” fields for the “Local (‘Left’)” host.

See Table 1-25, “Field and Menu Options for Configuring a VPN Connection,” on page 55 for what to enter on the screen. Work with the user who needs to make the VPN connection to make sure the information matches exactly on both ends.

▼ *To Configure VPN [Expert]*

To enable VPN, make sure that IPsec is also enabled. For details about the information you need to complete this screen, see Table 1-25, “Field and Menu Options for Configuring a VPN Connection,” on page 55, if needed.

1. Go to Configuration>Network>VPN Connections in Expert mode.

   The VPN Connections screen appears.

2. To edit a VPN connection, select the name, and click “Edit.”
3. To add a VPN Connection, click “Add.”

   The “New/Modify Connection” dialog box appears.

4. Enter any descriptive name you choose for the connection in the “Connection Name” field.
5. Select either ESP or “AH” from the “Authentication Protocol” pull-down menu.
6. Select either “Ignore, “Add,” or “Start” from the “Boot Action pull-down menu.
7. Select “Shared Secret” or “RSA Public Keys” from the “Authentication Method” pull-down menu.
8. Set up the right and left hosts by doing the following steps.
   a. Enter the name of the host in the “ID” field.
   b. Enter the IP address of the host in the “IP Address” field.
   c. Enter the IP address of the router through which the host’s packets reach the Internet in the “NextHop” field.
   d. Enter the netmask for the subnet in the “Subnet Mask” field.
   e. If “RSA Key” is selected, generate the key for the OnSite (left host) and find out the key from the remote gateway (where the right host resides). If desired, use copy and paste to enter the key in the “RSA Key” field.
   f. If “Shared Secret” is selected, enter the shared secret in the “Pre-Shared Secret” field.
   g. Click OK.

9. Click “apply changes.”

Configuration>Network>SNMP

Selecting Configuration>Network>SNMP in Expert mode brings up the screen shown in the following figure.

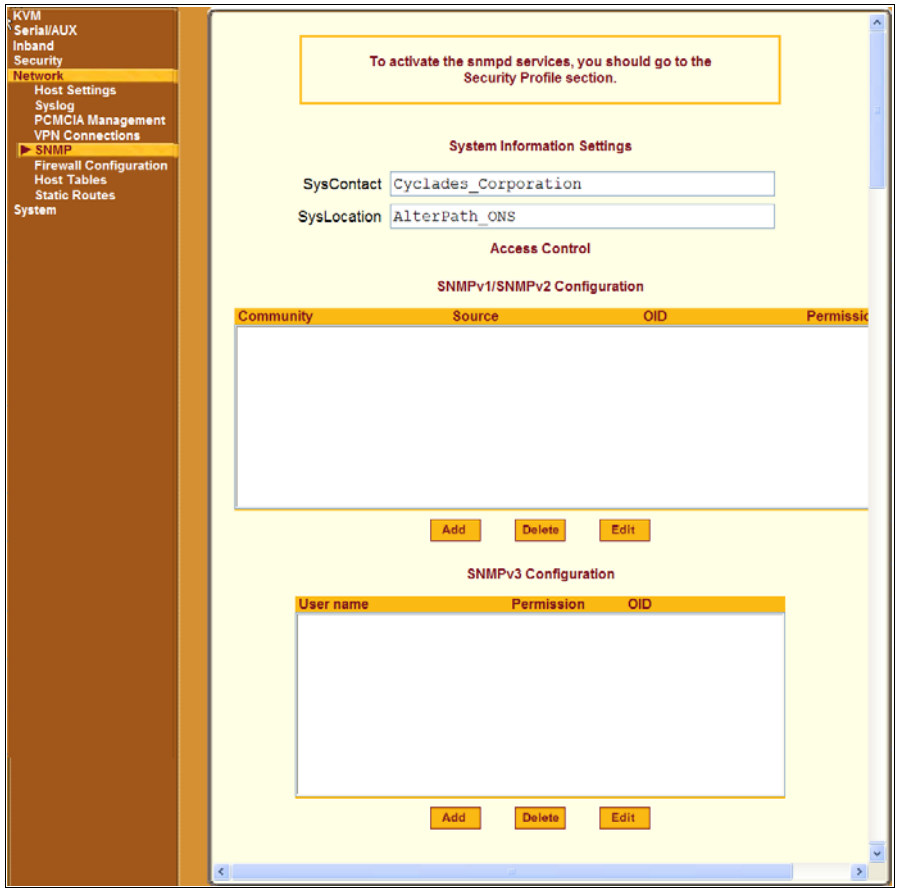


Figure 6-83: Web Manager Configuration>Network>SNMP Screen

An administrative user can use this screen to enable notifications about significant events or traps to be sent from the OnSite to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager.

The values you need to complete the screen and associated dialog boxes are explained in the following table.

Table 6-25: Fields and Menu Options for SNMP Configuration

Field or Menu Option	Description
SysContact	The email address of the OnSite's administrator, for example, `onsite_admin@cyclades.com`.
SysLocation	The physical location of the OnSite.
Community	SNMP v1 and v2 only. The community name is sent in every communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under "Permission": either read only or read write. The most common community is "public" and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the OnSite.
Source	SNMP v1 and v2 only. Valid entries are "default" or a subnet address, for example, `193.168.44.0/24`.
OID	Object Identifier. Each managed object has a unique identifier.
Permission	Select the permission type: Read Only - Read-only access to the entire MIB (Management Information Base) except for SNMP configuration objects. Read/Write - Read-write access to the entire MIB except for SNMP configuration objects.
User Name and Password	SNMP v3 only.

The OnSite SNMP agent supports SNMP v1, v2 and v3. To use SNMP v1 or v2, you need to specify a community name, source IP address or range of addresses, an object ID (OID), and permission (read-write or read-only). SNMP v3 requires: user name, password, OID, and permission.

Clicking the “Add” or “Edit” buttons under “SNMPv1/SNMPv2 Configuration” brings up the New/Modify SNMP v1 v2 Configuration” dialog box, as shown in the following figure.

Figure 6-84: “New/Mod SNMP v1 v2” Configuration Dialog Box

Clicking the “Add” or “Edit” buttons under “SNMPv3 Configuration” brings up the New/Modify SNMP v3 Configuration” dialog box, as shown in the following figure.

Figure 6-85: “New/Mod SNMP v3” Configuration Dialog Box

In addition to configuring the SNMP screen and the associated dialog boxes, the administrative user must do the following:

- Ensure that the SNMP service is activated
- Configure one or more serial ports to send SNMP traps.

The related tasks are listed in the following table.

Table 6-26: Tasks for Configuring SNMP

Task	Where Documented
Enable SNMP.	"To Configure SNMP [Expert]" on page 326
Configure one or more serial ports to send SNMP traps.	"To Configure a Trigger for SNMP Trap Notification for Serial Ports Expert]" on page 272

▼ *To Configure SNMP [Expert]*

1. Go to Configuration>Networks>SNMP in Expert mode.

   The SNMP screen appears.

2. To enable any version of SNMP, do the following:

   - To add an SNMPv1/SNMP2 entry, press the "Add" button under the "SNMPv1/SNMPv2 Configuration" table.
   - To add an SNMPv3 entry, press the "Add" button at the bottom of the "SNMPv3" table.

   The "New/Modify SNMP Daemon Configuration" dialog box appears.

3. To edit any SNMP configuration, do the following steps.

   a. To edit an SNMPv1/SNMP2 entry, select the entry from the "SNMPv1/SNMPv2 Configuration" list and click the "Edit" button.

   b. To edit an SNMPv3 entry, select an entry from the "SNMPv3" list and click the "Edit" button.

   The "New/Modify SNMP Daemon Configuration" dialog box appears.

4. For SNMP v1 or v2 configuration, enter or change the following information:

   a. Enter the community name in the "Community" field.

   b. Enter the source IP address or range of IP addresses in the "Source" field.

5. For SNMP v3 configuration, enter or change the following information:

a. Enter the user name in the “User name” field.

b. Enter the password in the “Password” field.

6. For any version of SNMP, do the following steps.

a. Enter the unique object identifier for the object in the “OID” field.

b. Choose “Read Only” or “Read/Write” from the “Permission” field.

7. Click OK.

8. Click “apply changes.

Configuration>Network>Firewall Configuration

Selecting Configuration>Network>Firewall Configuration in Expert mode brings up the screen shown in the following figure.

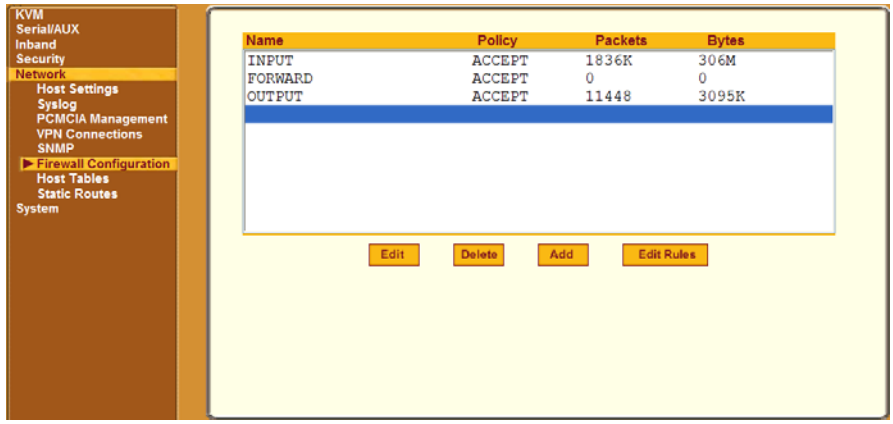


Figure 6-86: Web Manager Configuration>Network> Firewall Configuration Screen

An administrative user can use the Firewall Configuration screen to enable the OnSite to act like a firewall by filtering packets coming to and leaving the OnSite, allowing and disallowing packets according to rules you define.

Packet filtering relies on chains and rules being defined. See “Packet Filtering on the OnSite” on page 65 for details.

Each entry in the list on the Firewall Configuration screen represents a chain with a set of rules.

The list by default has three built-in chains, as shown in the previous figure. The chains accept all INPUT, FORWARD, and OUTPUT packets. An administrative user can use the “Edit,” “Delete,” “Add,” and “Edit Rules” buttons on the screen to do the following to configure packet filtering:

- Edit default chains
- Delete user-added chains
- Add new chains
- Edit rules for chains

Firewall Configuration: Editing Chains

If one of the default chains is selected and the “Edit” button is pressed under Configuration>Network>Firewall Configuration in Expert mode, the “Edit Chain” dialog box shown in the following figure appears.

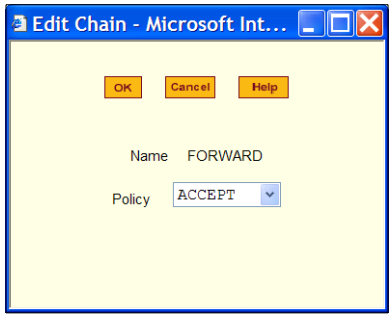


Figure 6-87: Firewall Configuration “Edit Chain” Dialog Box

Only the policy can be edited for a default chain. The options are “ACCEPT,” and “DROP.”

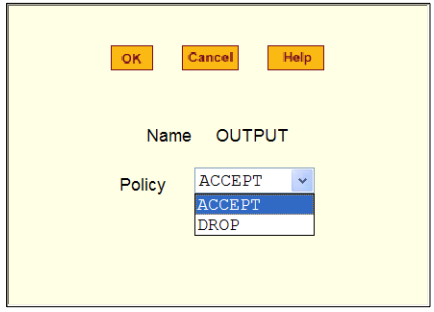


Figure 6-88: Firewall Configuration “Edit Chain” Policy Options

User-defined chains cannot be edited. If a user-defined chain is selected for editing, the message shown in the following figure appears.

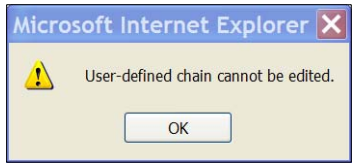


Figure 6-89: Firewall Configuration “User-defined Chain” Message

Firewall Configuration: Deleting Chains

If one of the default chains is selected and the “Delete” button is pressed under Configuration>Network>Firewall Configuration in Expert mode, the chain is deleted.

Default chains cannot be deleted. If a user-defined chain is selected and the “Delete” button is pressed, the message shown in the following figure appears.

Figure 6-90: Firewall Configuration “Delete Default Chain” Dialog Box

Firewall Configuration: Adding Chains

If the “Add” button is pressed under Configuration>Network>Firewall Configuration in Expert mode, the “Add Chain” dialog box shown in the following figure appears.

Figure 6-91: Firewall Configuration “Add Chain” Dialog Box

Adding a chain only creates an named entry for the chain. Rules must also be configured for the chain after it is added to the list of chains.

Firewall Configuration: Editing Rules

If the “Edit Rules” button is pressed under Configuration>Network>Firewall Configuration in Expert mode, a screen appears with a list of headings like the one shown in the following figure. (The example shows the OUTPUT chain selected for editing, which has no rules defined.)

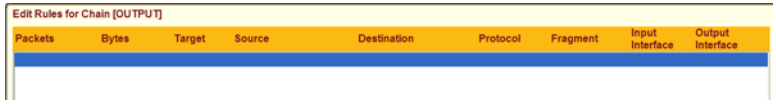


Figure 6-92: Firewall Configuration “Edit Rules for *chain_name*” Screen

The buttons shown in the following figure appear at the bottom of the screen.

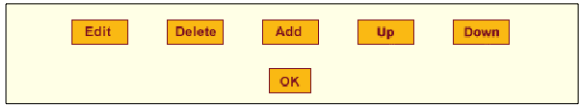


Figure 6-93: Firewall Configuration “Edit Rules for *chain_name*” Buttons

When the “Add” button is pressed, the “Add Rule” dialog box appears. When a rule is selected and the “Edit” button is pressed, the “Edit Rule” dialog box appears. When a rule is selected, pressing the “Up,” and “Down” buttons moves the rule up and down the list.

Firewall Configuration: Options on the “Add Rule” and “Edit Rule” Dialog Boxes

The “Add Rule” and “Edit Rule” dialog boxes under Configuration> Network>Firewall Configuration in Expert mode have the fields and options shown in the following figure.

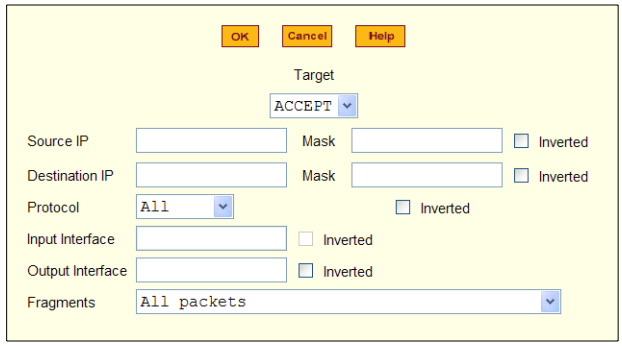


Figure 6-94: Firewall Configuration “Add Rule” and “Edit Rule” Dialog Boxes

Firewall Configuration: Inverted Checkboxes

If the “Inverted” checkbox is checked on any line in the “Add Rule” or “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode, the target action is performed on packets that do not match any of the criteria specified in that line when any other specified criteria are also met.

For example, if you select DROP as the target action, check “Inverted” on the line with a source IP address specified, and do not specify any other criteria in the rule, any packets arriving from any other source IP address than the one specified are dropped.

Firewall Configuration: Target Pull-down Menu Options

The “Target” on the “Add Rule” and “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode is the action to be performed on an IP packet that matches all the criteria specified in a rule.The default target pull-down menu is shown in the following figure.

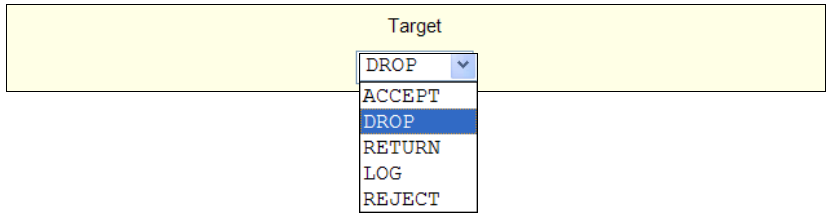


Figure 6-95: Firewall Configuration “Add Rule” and “Edit Rule” Target Menu Options

If the “LOG” and “REJECT” targets are selected, additional fields appear as described under “LOG Target” on page 242 and “REJECT Target” on page 243.

Source or Destination IP and Mask

If you fill in the “Source IP” field on the “Add Rule” and “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode, incoming packets are filtered for the specified IP address. If you fill in the “Destination IP” field, outgoing packets are filtered for the specified IP address.

If you fill in either “Mask” field, incoming or outgoing packets are filtered for IP addresses from the network in the specified netmask.

The source and destination IP and related fields are shown in the following figure.

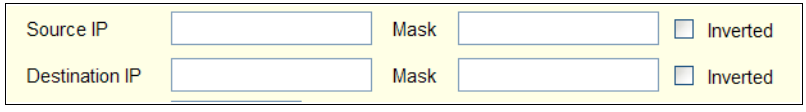


Figure 6-96: Firewall Configuration “Add Rule” and “Edit Rule” Source and Destination IP and Mask Fields

Firewall Configuration: Protocol

An administrative user can select a protocol for filtering on the “Add Rule” and “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode. The “Protocol” pull-down menu is shown in the following figure.

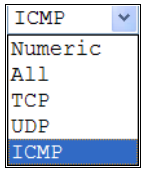


Figure 6-97: Firewall Configuration “Add Rule” and “Edit Rule” Protocol Menu Options

The additional fields that appear for each protocol are explained in the following sections.

Firewall Configuration: Numeric Protocol Fields

If Numeric is selected as the protocol when specifying a rule in the “Add Rule” and “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode, a text field appears to the right of the menu for the desired number, as shown in the following figure.

Figure 6-98: Firewall Configuration “Add Rule” and “Edit Rule” Numeric Protocol Fields

Firewall Configuration: TCP Protocol Fields

If TCP is selected as the protocol when specifying a rule in the “Add Rule” and “Edit Rule” dialog boxes under Configuration>Network>Firewall Configuration in Expert mode, the additional fields shown in the following figure appear at the bottom of the screen.

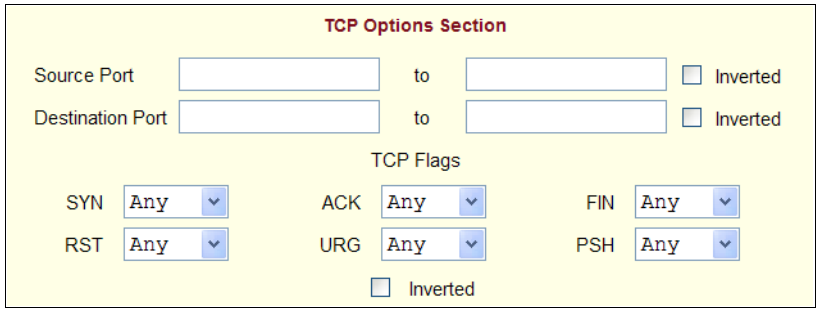


Figure 6-99: Firewall Configuration “Add Rule” and “Edit Rule” TCP Protocol Fields and Menu Options

The following table defines the fields and menu options in the “TCP Options Section.”

Table 6-27: TCP Options Fields and Menu Options on the Firewall Configuration Screen

Field/Menu Option	Definition
Source Port - OR - **Destination Port** -AND- **to**	A source or destination port number for filtering in the “Source Port” or “Destination Port” field. If a second number is entered in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.
TCP Flags	The TCP flags “SYN” (synchronize), “ACK” (acknowledge), “FIN” (finish), “RST” (reset), “URG” (urgent) or “PSH” (push) cause TCP packets to be filtered for the specified flag and the selected condition, either “Any,” “Set,” or “Unset.”

Firewall Configuration: UDP Protocol Fields

If UDP is selected as a protocol when specifying a rule, the additional fields shown in the following figure appear at the bottom of the screen.

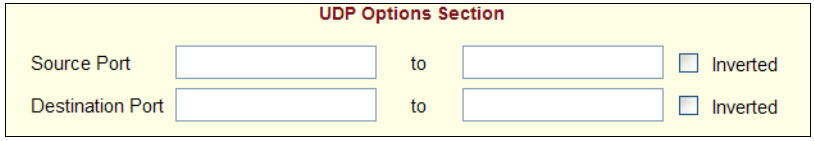


Figure 6-100: Firewall Configuration “Add Rule” and “Edit Rule” UDP Protocol Fields

The following table defines the fields in the UDP Options Section.

Table 6-28: UDP Options Fields in the Firewall Configuration Screen

Field	Definition

Table 6-28: UDP Options Fields in the Firewall Configuration Screen

Source Port - OR - **Destination Port**	A source or destination port number for filtering in the “Source Port” or “Destination Port” field.
-AND- **to**	A source or destination port number for filtering in the “Source Port” field. If a second number is entered the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.

Firewall Configuration: ICMP Protocol Fields

If ICMP is selected as a protocol when specifying a rule, the ICMP Type pull-down menu appears in the ICMP Options Section at the bottom of the Firewall Configuration screen. The following figure shows the options.

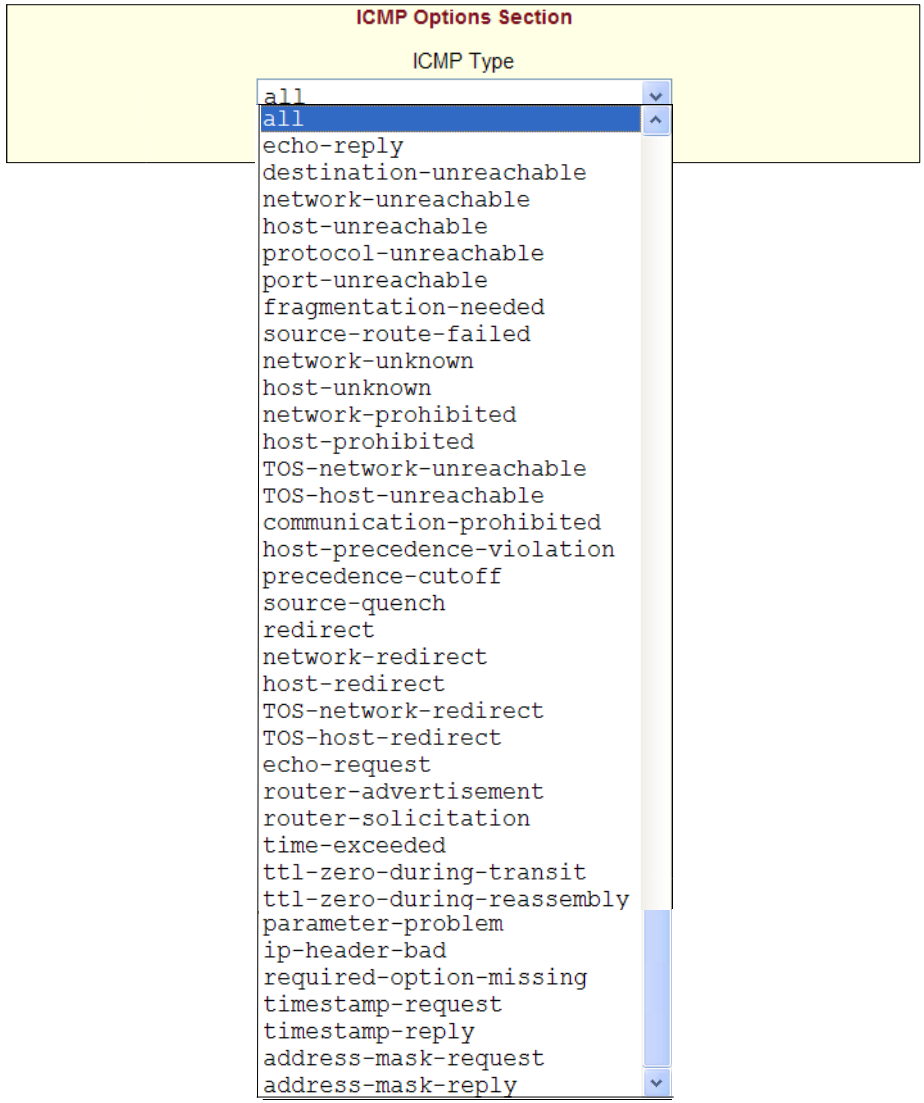


Figure 6-101: Firewall Configuration “Add Rule” and “Edit Rule” ICMP Type Menu Options

Firewall Configuration: Input Interface, Output Interface, and Fragments

If an interface (such as `eth0` or `eth1`) is entered in the “Input Interface” field, incoming packets are filtered for the specified interface. If an interface is entered in the “Output Interface” field, outgoing packets are filtered for the specified interface. The input and output interface fields are shown in the following figure along with the options on the “Fragments” pull-down menu.

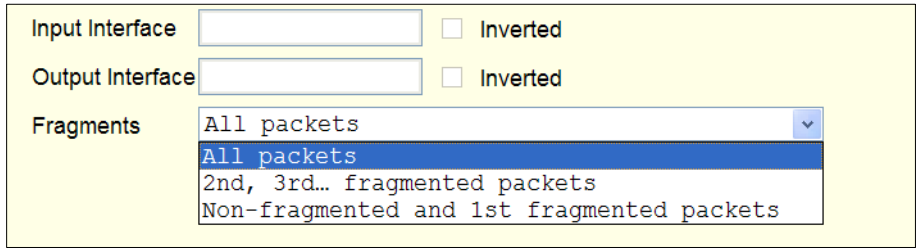


Figure 6-102: Firewall Configuration “Add Rule” and “Edit Rule” Input and Output Interface Fields and Fragments Menu Options

The following table defines the fields in the above figure.

Table 6-29: Input and Output Interface and Fragment Options in the Firewall Configuration Screen

Field	Definition
Input Interface	The input interface (eth*N*) for the packet
Output Interface	The output interface (eth*N*) for the packet
Fragments	The types of packets to be filtered: All packets 2nd, 3rd... fragmented packets Non-fragmented and 1st fragmented packets

Firewall Configuration: LOG Target

Note: If you select “LOG” from the “Target” field, the fields and menus shown in the following figure appear in the “LOG Options Section” at the bottom of the screen.

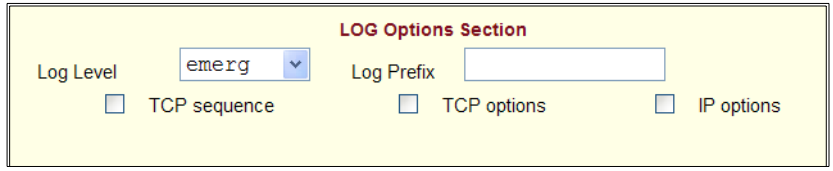


Figure 6-103: Firewall Configuration “Add Rule” and “Edit Rule” LOG Target Fields

The following table defines the menu options, field, and checkboxes in the “LOG Options Section.”

Field or Menu Name	Definition
Log Level	One of the options in the pull-down menu: emerg alert crit err warning notice info debug
Log Prefix	The prefix is included in the log entry.
TCP Sequence	Includes the TCP sequence in the log.
TCP Options	Includes TCP options in the log.
IP Options	Includes IP options in the log.

Firewall Configuration: REJECT Target

If REJECT is selected from the Target pull-down menu, the following pull-down menu appears

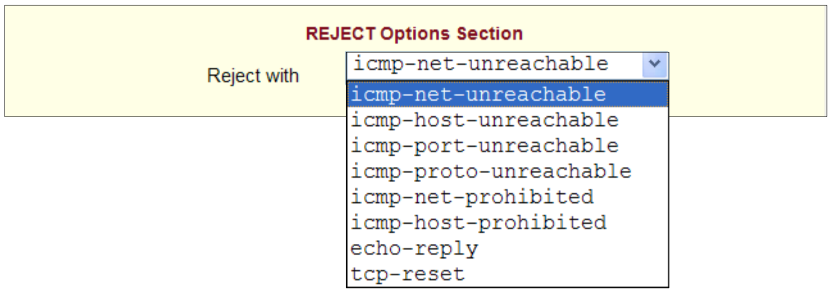


Figure 6-104: Firewall Configuration "Add Rule" and "Edit Rule" REJECT Target Menu Options

Any "Reject with" option causes the input packet to be dropped and a reply packet of the specified type to be sent.

Firewall Configuration Procedures

The following table has links to the procedures for defining packet filtering:

To Add a Chain [Expert]	Page 339
To Edit a Chain [Expert]	Page 340
To Edit a Rule [Expert]	Page 341
To Add a Rule [Expert]	Page 341

▼ *To Add a Chain [Expert]*

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.

   The Firewall Configuration screen appears.

2. Click "Add."

   The "Add Chain" dialog box appears.

3. Enter the name of the chain to be added in the "Name" field and then click OK.

Note: Spaces are not allowed in the chain name.

The name of the new chain appears in the list.

4. Finish defining the chain by adding one or more rules, as described in to “To Add a Rule” on page 245.

▼ *To Edit a Chain [Expert]*

Perform this procedure if you want to change the policy for a default chain.

Note: User-defined chains cannot be edited. If you want to rename a chain you added, delete it and create a new one.

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
2. Select one of the default chains from Chain list, and then click the “Edit” button.

   If you select a user-defined chain, the dialog box shown in the following figure appears.

   If you select one of the default chains, the “Edit Chain” dialog box appears.
3. Select the desired policy from the Policy pull-down menu, and then click OK.
4. Click “apply changes.”
5. To edit any rules for this chain, go to “To Edit a Rule.”

▼ To Edit a Rule [Expert]

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
2. Select the chain whose rule you want to edit from Chain list, and then click the “Edit Rules” button.

   The “Edit Rules” screen appears.
3. Select the rule to be edited from the Rules list, and then click the “Edit” button.

   The “Edit Rule for *chain_name*” dialog box appears.
4. Modify the rule as desired.

   For definitions of the fields in this screen see “Configuration>Network>Firewall Configuration” on page 327, if needed.
5. Click OK.
6. Click “apply changes.”

▼ To Add a Rule [Expert]

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
2. Select the chain to which you want to add a rule from Chain list, and then click the “Edit Rules” button.
3. Click the “Add Rule” button.

   The “Add Rule for *chain_name*” dialog box appears.
4. Configure the rule as desired.

   For definitions of the fields in this screen see “Configuration>Network>Firewall Configuration” on page 327, if needed.
5. Click OK.
6. Click “apply changes.”

Configuration>Network>Host Tables

Selecting Configuration>Network>Host Tables in Expert mode brings up the screen shown in the following figure.

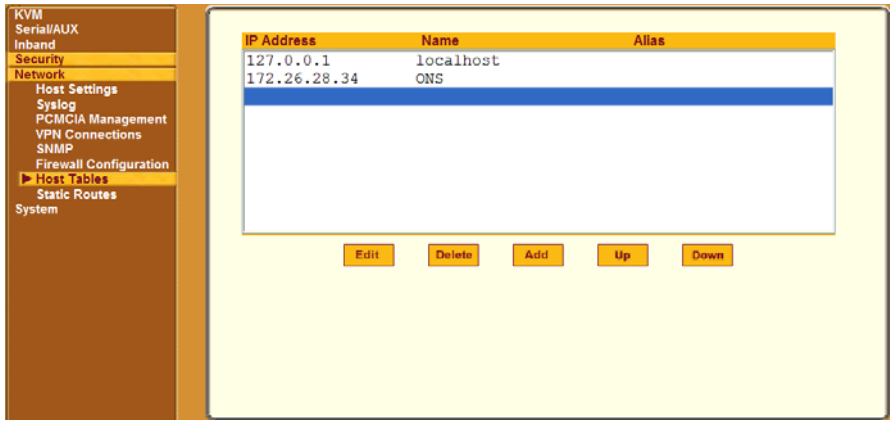


Figure 6-105: Web Manager Configuration>Host Tables Screen

An administrative user can use the screen to add, and edit or delete hosts.

▼ *To Define the OnSite's IP Address and Hostname [Expert]*

1. Go to Configuration>Network>Host Table in Expert mode.

   The Host Table screen appears.

2. To edit a host, select the host IP address from the Host Table and then click the "Edit" button. (If needed, use the "Up" and "Down" buttons to navigate through the list.)

3. To add a host, click the "Add" button.

   The "host table" dialog box appears.

4. Enter the new or modified host address in the "IP Address field," and the host name in the "Name" field, and then click "OK."

5. To delete a host, select the host you wish to delete and click "Delete."

6. Click "apply changes."

Configuration>Network>Static Routes

Selecting Configuration>Network>Static Routes in Expert mode brings up the screen shown in the following figure.

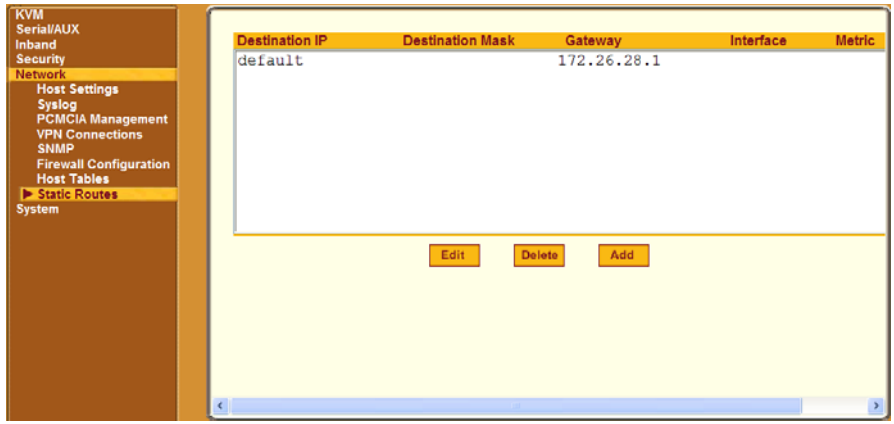


Figure 6-106: Web Manager Configuration>Network Static Routes Screen

An administrative user can use the screen to manually add static routes or edit or delete existing routes.

Clicking the “Edit” or “Add” buttons brings up a screen like the one shown in the following figure. The example shows the fields and menus that appear when the “Default” route type is selected in the “Route” pull-down menu.

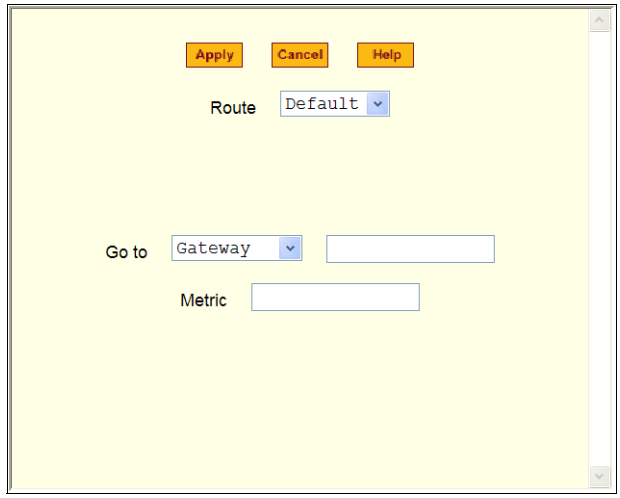


Figure 6-107: Static Routes “Add” and “Edit” Fields and Menu Options—Default Route

The following figure shows the fields and menus that appear when the “Network” route type is selected in the “Route” pull-down menu.

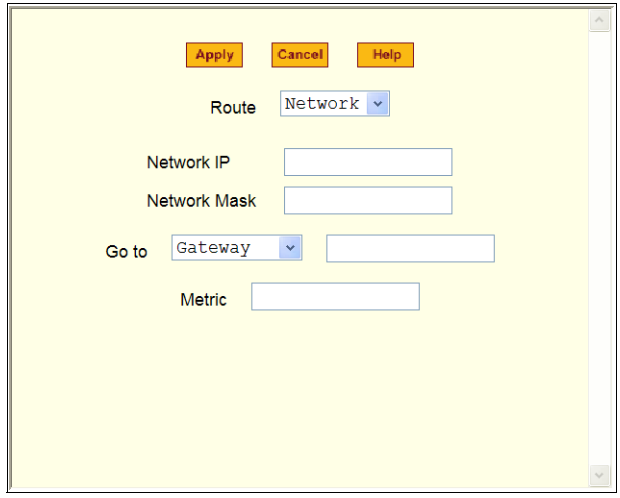


Figure 6-108: Static Routes “Add” and “Edit” Fields and Menu Options—Network Route

The following figure shows the fields and menus that appear when the “Host” route type is selected in the “Route” pull-down menu.

Figure 6-109: Static Routes “Add” and “Edit” Fields and Menu Options—Host Route

The following table describes the fields that appear when you select the “Edit” or “Add” buttons.

Table 6-30: Fields and Menus for Configuring Static Routes

Field or Menu Name	Definition
Route	Choices are “Default,” “Network,” or “Host.”
Network IP	This field appears only when “Network” is selected. Type the address of the destination network.
Network Mask	Appears only when “Network” is selected. Type the netmask of the destination network.
Host IP	Appears only when “Host” is selected. Type the IP address of the destination host.
Go to	Choices are “Gateway” or “Interface.”
[*Adjacent field*]	Type the IP address of the gateway or the name of the interface.
Metric	Type the number of hops to the destination.

▼ *To Configure Static Routes [Expert]*

See Table 6-30, “Fields and Menus for Configuring Static Routes,” on page 345 if needed.

1. Go to Configuration>Network>Static Routes in Expert Mode.

   The Static Routes screen appears.

   - To edit a static route, select a route from the “Static Routes” list, and then select the “Edit” button.
   - To add a static route, select the “Add” button from the screen.

   The system invokes the New/Modify Route dialog box.

2. Choose “Default,” “Network,” or “Host” from the “Route” pull--down menu.
3. If you selected “Network, do the following steps.
   a. Enter the IP address of the destination network in the “Network IP” field.
   b. Enter the netmask of the destination network in the “Network Mask” field.
4. If you selected “Host,” type the IP address of the destination host in the “Host IP” field.
5. Select “Gateway” or “Interface” from the “Go to” pull-down menu and enter the address of the gateway or the name of the interlace in the adjacent field.
6. Click “apply changes.”

Configuration>System

Selecting Configuration>System in Expert mode brings up three options in the left menu as shown in the following figure.

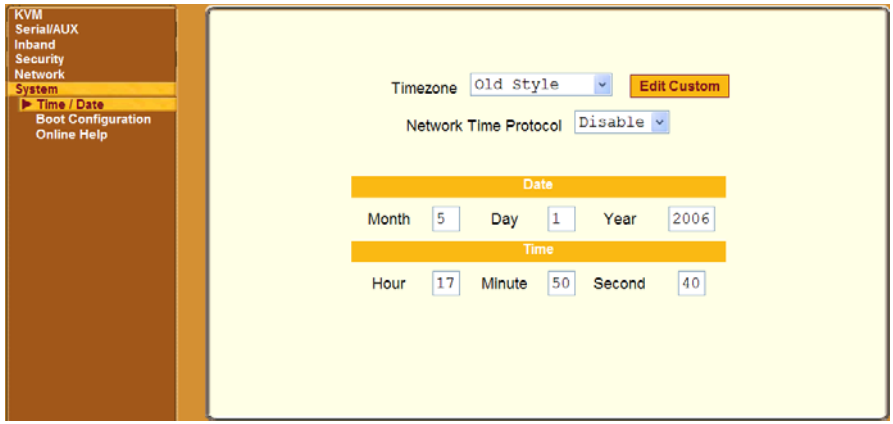


Figure 6-110: Web Manager Configuration>System Menu Options

An administrative user can use the Network screens to configure network-related features, as described in the following sections:

- “Configuration>System>Time/Date” on page 347
- “Configuration>System>Boot Configuration” on page 351
- “Configuration>System>Online Help” on page 355

Configuration>System>Time/Date

When Configuration>System Time/Date is selected in Expert mode, the screen in Figure 6-110 appears.

An administrative user can use the Time/Date screen to configure the timezone and the OnSite’s time and date in one of the following two ways:

- By manually entering the current date and time.
- By configuring an NTP server

  Enabling Network Time Protocol (NTP) and configuring the IP address of an NTP server synchronizes the OnSite’s system clock with the NTP server, which maintains the true time (the average of many high-accuracy clocks around the world).

If “Disable” is selected from the Network Time Protocol menu, manual configuration includes configuring the timezone and manually entering the date and time.

Configuring the timezone is done in either one of the two ways listed in the following list.

- Click the “Edit Custom” button

  See “Custom Editing the Time Zone” on page 348.

- Select from the “Timezone” menu

  See “Selecting From the Timezone Menu” on page 349.

When the Time/Date option is selected, if “Old Style” is selected on the “Timezone” menu, the following window appears.

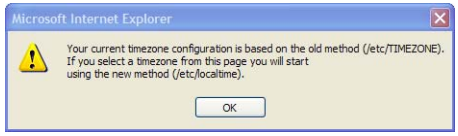


Figure 6-111: Time/Date Window

Custom Editing the Time Zone

Clicking the “Edit Custom” button brings up the window shown in the following figure.

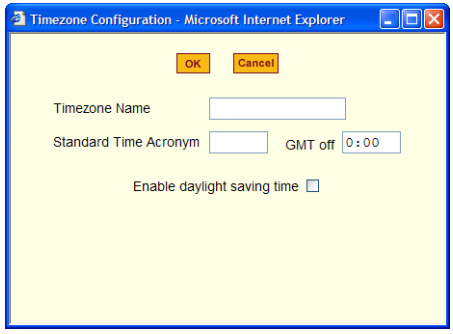


Figure 6-112: Timezone “Edit Custom” Screen

Selecting From the Timezone Menu

The “Timezone” menu is shown in the following figure.

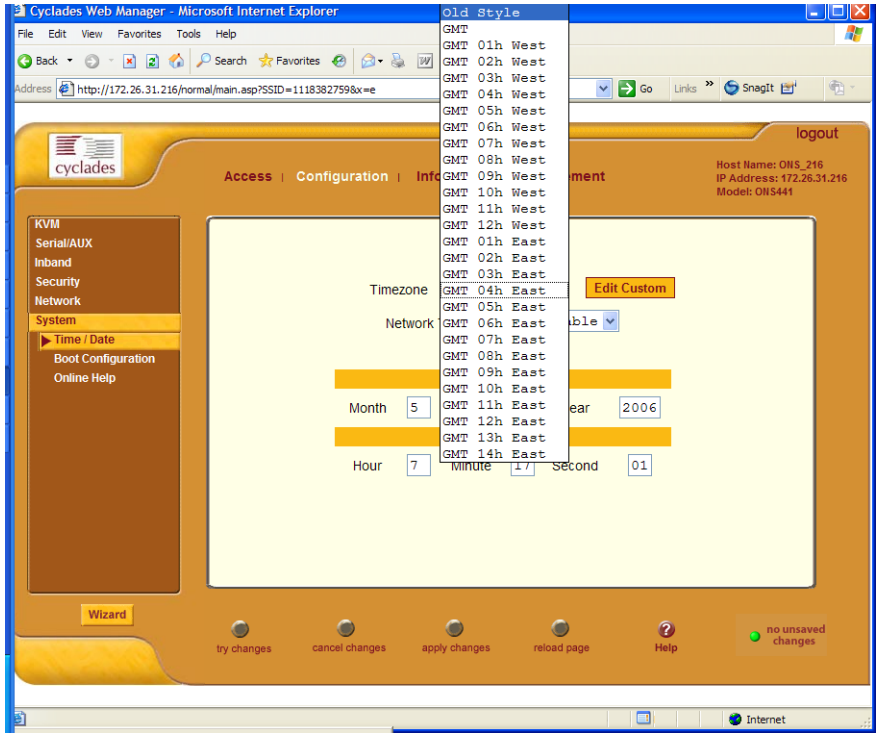


Figure 6-113: Web Manager>Configuration>System>Time/Date Menu

▼ *To Configure the Time Zone [Expert]*

1. Go to Configuration>System>Time/Date in Expert mode.

   The Time/Date screen appears.

2. Do one of the following to configure the timezone.

   a. Select a timezone from the “Enable Timezone:” pull-down menu.

   b. Click the “Edit Custom from the “Enable Timezone:” pull-down menu, and do the following steps.

      i. Enter the name of the timezone in the “Timezone Name” field.

ii. Enter an acronym in the “Standard Time Acronym” field.

iii. Enter the number of hours and minutes off Greenwich Mean Time in the “GMT off” field.

iv. If desired, check the “Enable daylight saving time” checkbox.

v. Click OK.

3. Go to one of the procedures listed below to configure the time.

- “To Configure Time and Date [Expert]” on page 350.
- “To Configure Time and Date [Expert]” on page 350

Enabling NTP

If “Enable” is selected from the Network Time Protocol menu, a screen like the one shown in the following figure appears.

Figure 6-114:NTP Enable Screen

▼ *To Configure Time and Date [Expert]*

1. Perform the procedure under “To Configure the Time Zone [Expert]” on page 349.

2. To configure an NTP server, do the following steps.

a. Select “Enable” from the Network Time Protocol menu.

The “NTP Server” field appears.

b. Type the IP address of the NTP server in the “NTP Server” field.

3. To configure time and date manually, do the following steps.
   a. Select “Disable” from the Network Time Protocol menu.

      The “Date” and “Time” fields appear.

   b. Enter the month, day, and year under the “Date” header.
   c. Enter the hour, minute, and second under the “Time” header.
4. Click “apply changes.”

Configuration>System>Boot Configuration

Selecting Configuration>System>Boot Configuration in Expert mode brings up a screen like the one shown in the following figure.

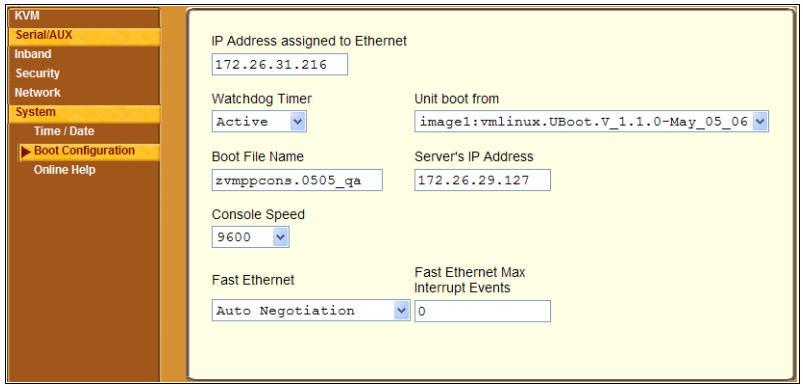


Figure 6-115: Web Manager Configuration>System>Boot Configuration Screen

On the Boot Configuration screen under Configuration>System in Expert mode, an administrative user can redefine the location from which the OnSite boots. By default, the OnSite boots from a boot file in the on-board Flash memory. Booting from the resident software is recommended except when troubleshooting boot problems. The differences between booting from a local copy of the software image and booting from the network are explained in the following sections.

For more details, also see“Boot File Location Information” on page 372.

Local Boot Options

To understand the “Unit boot from” options, the administrative user need to understand how the OnSite handles software upgrades:

- The OnSite initially boots from a software image referred to as “image1.”
- The first time you download and install a new software version from Cyclades, the new image is stored as “image2” in the Flash memory and the configuration is changed to boot the OnSite from “image 2.”
- The second time you download a new software version, the latest image is stored as “image 1,” and the OnSite configuration is changed to boot from “image1.”
- Subsequent downloads are stored following the same pattern, alternating “image1” with “image2.”

In the “Unit boot from” pull-down menu, the entry for the *current* image is selected by default. The word “image” is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. The menu item has the following format:

`image1:zvmppcons.v`*`version_number`*

The entry for the first release of the software, which is installed in the image1 area, is:

`image1:zvmppcons`.v100

After one or more software upgrades have been performed, a second image also appears in the menu, for example:

`image1:zvmppcons`.v100

`image2:zvmppcons`.v101

If, for any reason, the system should boot from another image than the one currently selected, the administrative user can select that image from the “Unit boot from” menu.

Network Boot Options

Network boots are recommended only for troubleshooting or for possible downloads of new software images that can be stored in the on-board Flash memory, as described in “To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode” on page 572. See Appendix A, “Advanced Boot and

Backup Configuration Information” for where these advanced configuration options are described.

To boot from a boot server, the administrative user can select “Network” and configure a boot server.

For network boot to work, make sure the following prerequisites are done.

- A TFTP server must be available to the OnSite on the network.
- An upgraded OnSite boot image file must be downloaded from Cyclades and available on the boot server.
- The OnSite must have a fixed IP address and you must know the address.
- You must know the boot filename and the IP address of the TFTP server.

The boot-related options are described in the following table.

Table 6-31: Boot Configuration Fields and Options

Field or Value Name	Description
IP Address assigned to Ethernet	A new IP address for the OnSite.
Watchdog Timer	Whether the watchdog timer is active. If the watchdog timer is active, the OnSite reboots if the software crashes. See “Configuration>System>Boot Configuration” on page 351 for how the watchdog timer can be activated or deactivated.
Unit boot from	Choose one or more images and “Network” from the list.
Boot File Name	An alternative name for the boot file.
Server’s IP Address	The IP address for the boot server.
Console Speed	An alternative console speed from 4800 to 115200 (9600 is the default).

Table 6-31: Boot Configuration Fields and Options

Field or Value Name	Description
Fast Ethernet	The speed of the Ethernet connection: Auto Negotiation, 100 BaseT Half-Duplex, 100 BaseT Full-Duplex, 10 BaseT Half-Duplex, 10 BaseT Full Duplex.
Fast Ethernet Max Interrupt Events	An alternate number of maximum interrupt events to improve performance (0 is the default).

▼ *To Configure OnSite Boot [Expert]*

For more information about the fields in the "Boot Configuration" screen, see Table 6-31, if desired.

1. Go to Configuration>System>Boot Configuration in Expert mode.

   The Boot Configuration screen appears.

2. Enter the IP address of the OnSite in the "IP Address assigned to Ethernet" field.
3. Accept or change the selected option in the "Watchdog Timer" field.
4. Choose the desired image or "Network" from the "Unit boot from" menu.
5. Accept or change the filename of the boot program in the "Boot File Name" field.
6. If specifying network boot, do the following steps.
   a. Enter the IP address of the TFTP server in the "Server's IP Address" field.
   b. Select a console speed from the "Console Speed" pull-down menu to match the speed of the terminal you are using on the console port of the OnSite.
   c. Choose an Ethernet speed from the "Fast Ethernet" pull-down menu.
   d. Specify the maximum number of packets that the CPU handles before an interrupt in the "Fast Ethernet Max. Interrupt Events" field.
7. Click "apply changes."

Configuration>System>Online Help

Selecting Configuration>System>Online Help in Expert mode brings up a screen like the one shown in the following figure.

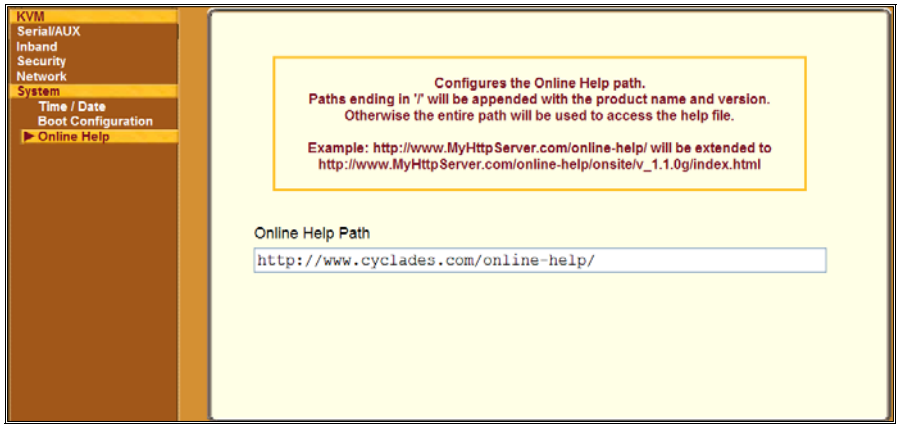


Figure 6-116: Web Manager Configuration>System>Online Screen

The Help button on the Web Manager locates the help files in the location that is configured here. By default, the OnSite help is located at the Cyclades web site at `http://www.cyclades.com/online-help/onsite/v_1.1.0`. The OnSite software expands the specified URL: `http://www.cyclades.com/online-help/`, adding the product name and version number `onsite/v_1.1.0`.

This screen allows the help files to be stored at another location. It may be useful, for example, if users cannot access the Cyclades website for whatever reason. If an OnSite administrator downloads the help files from the Cyclades ftp server onto another web server or other directory that is available to users, then the administrative user can change the URL in the “URL Prefix” field to point to the new location for the files.

Note: If the pathname ends with a slash (/), the Web Manager appends `onsite/v_1.1.0` to what is entered into the OnLine Help Path field. If you want to store the help files in a directory whose pathname does not use the above convention, make sure that the pathname entered in this field does not end with a slash.

▼ *To Configure a New Location for OnSite Help Files*

1. Download the compressed help file from `ftp.cyclades.com`.

   The pathname of the file is `ftp://ftp.cyclades.com/pub/cyclades/alterpath/onsite/doc/OnSite_online_hlp.zip`.

2. Extract the help files and put them into the desired directory under the web server's root directory on a web server that is accessible to the OnSite.

   For example the following command line would work on a computer running a UNIX-based operating system.

```
# cd $WEB_SERVER_ROOT/
# gunzip OnSite_online_hlp.zip
```

   By default, the compressed online help files are expanded under an `onsite` directory that is created the directory where the zip file is located.

   If desired, rename the `onsite` directory with another name of your choosing. For example, if you want to keep multiple versions of OnSite help from several releases, you could put them into directories whose names reflect the version number.

3. Log into the Web Manager as an administrative user, and go to Configuration>System>Online Help.

   The Help configuration screen appears.

4. In the "Online Help Path" field, enter the URL of the help files on the server where you installed them.

   The following example URL would work for a web server named `remoteadmin`.

5. Click “apply changes.”

Information

Under “Information” in Expert mode, four options appear in the left menu, as shown in the following figure.

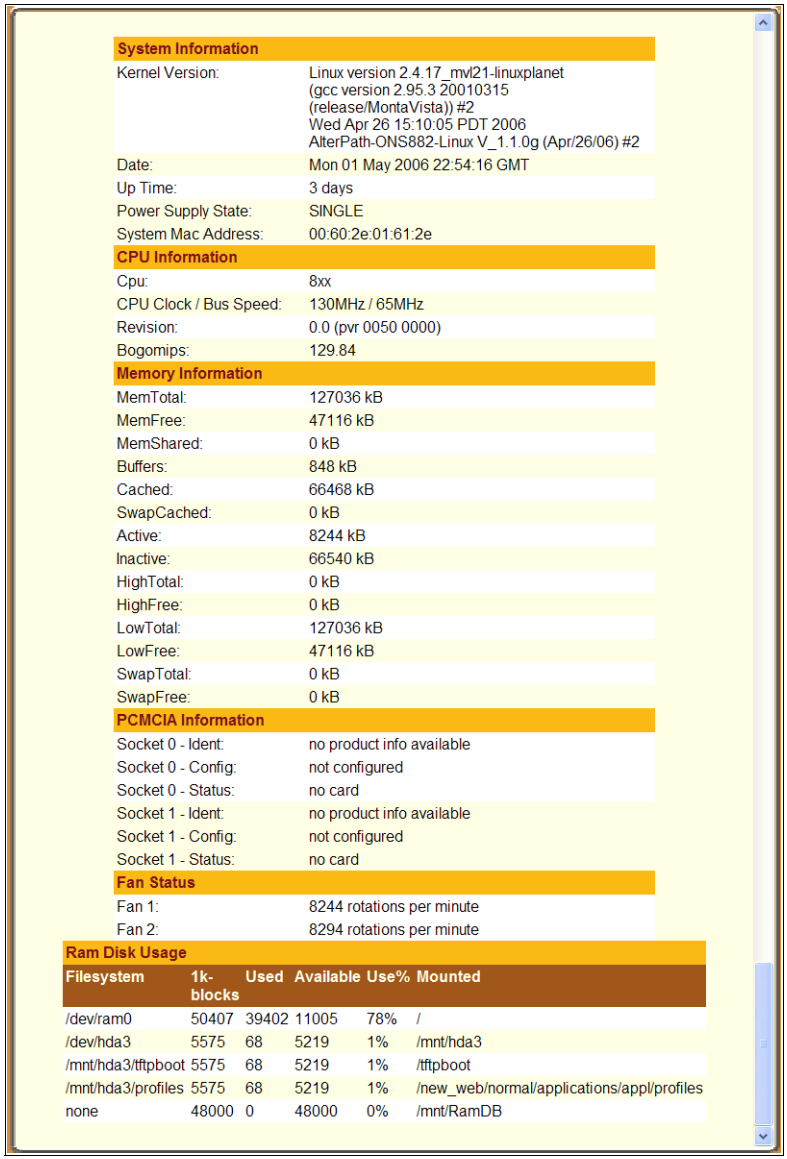
Figure 6-117: Web Manager Information Menu Options

An administrative user can use the Information menu options view various types of information, as described in the following sections.

- “Information>General” on page 358
- “Information>KVM User Status” on page 360
- “Information>Serial Ports Status” on page 361
- “Information>Serial Ports Statistics” on page 362

Information>General

Selecting Information>General in Expert mode brings up an information screen like the one in the following figure.



System Information	
Kernel Version:	Linux version 2.4.17_mvl21-linuxplanet (gcc version 2.95.3 20010315 (release/MontaVista)) #2 Wed Apr 26 15:10:05 PDT 2006 AlterPath-ONS882-Linux V_1.1.0g (Apr/26/06) #2
Date:	Mon 01 May 2006 22:54:16 GMT
Up Time:	3 days
Power Supply State:	SINGLE
System Mac Address:	00:60:2e:01:61:2e
CPU Information	
Cpu:	8xx
CPU Clock / Bus Speed:	130MHz / 65MHz
Revision:	0.0 (pvr 0050 0000)
Bogomips:	129.84
Memory Information	
MemTotal:	127036 kB
MemFree:	47116 kB
MemShared:	0 kB
Buffers:	848 kB
Cached:	66468 kB
SwapCached:	0 kB
Active:	8244 kB
Inactive:	66540 kB
HighTotal:	0 kB
HighFree:	0 kB
LowTotal:	127036 kB
LowFree:	47116 kB
SwapTotal:	0 kB
SwapFree:	0 kB
PCMCIA Information	
Socket 0 - Ident:	no product info available
Socket 0 - Config:	not configured
Socket 0 - Status:	no card
Socket 1 - Ident:	no product info available
Socket 1 - Config:	not configured
Socket 1 - Status:	no card
Fan Status	
Fan 1:	8244 rotations per minute
Fan 2:	8294 rotations per minute

Ram Disk Usage

Filesystem	1k-blocks	Used	Available	Use%	Mounted
/dev/ram0	50407	39402	11005	78%	/
/dev/hda3	5575	68	5219	1%	/mnt/hda3
/mnt/hda3/tftpboot	5575	68	5219	1%	/tftpboot
/mnt/hda3/profiles	5575	68	5219	1%	/new_web/normal/applications/appl/profiles
none	48000	0	48000	0%	/mnt/RamDB

Figure 6-118: Web Manager Information>General Screen

Administrative users can view information in the following categories on the screen shown in Figure 6-118:

- System (kernel version, date, uptime, power supply state, system MAC address)
- CPU (number, clock speed, revision, bogomips)
- Memory (total, free, shared, buffers, cached, swapcached, active, inactive, high total, high free, low total, low free, swap total, swap free)
- PCMCIA (for each slot, the following about each inserted card: identity and configuration status)
- Fan Status (rotations per minute for each of the two fans)
- Ram Disk Usage (filesystem data)

▼ *To View System, CPU, Memory, Fan, and RAMDISK Information [Expert]*

1. Go to Information>General in Expert mode.

   The General screen appears.

2. Scroll down to view all the information.
3. When you are done, click another Web Manager option.

Information>KVM User Status

Selecting Information>KVM User Status in Expert mode brings up the screen shown in the following figure.

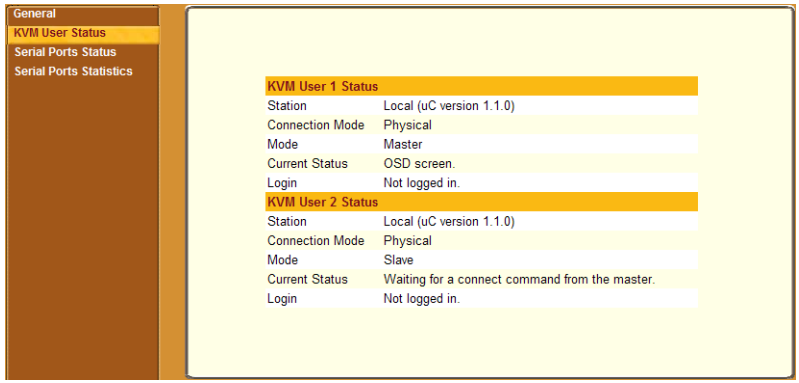


Figure 6-119: Web Manager Information>KVM User Status Screen

Administrative users can use this screen to view the status of the one or two users who may be connected to KVM ports. See “Understanding KVM Port Permissions” on page 32 for details about how many KVM users can be connected at the same time, either locally or remotely.

Status is given for KVM users in the following categories:

- Station
- Connection mode
- Mode
- Current status
- Login

▼ *To View KVM User Status [Expert]*

1. Go to Information>KVM User Status in Expert mode.

   The KVM User Status view screen appears:

2. View the status.
3. When you are done, click on the name of another screen.

Information>Serial Ports Status

Selecting Information>Serial Port Status in Expert mode brings up the screen shown in the following figure.

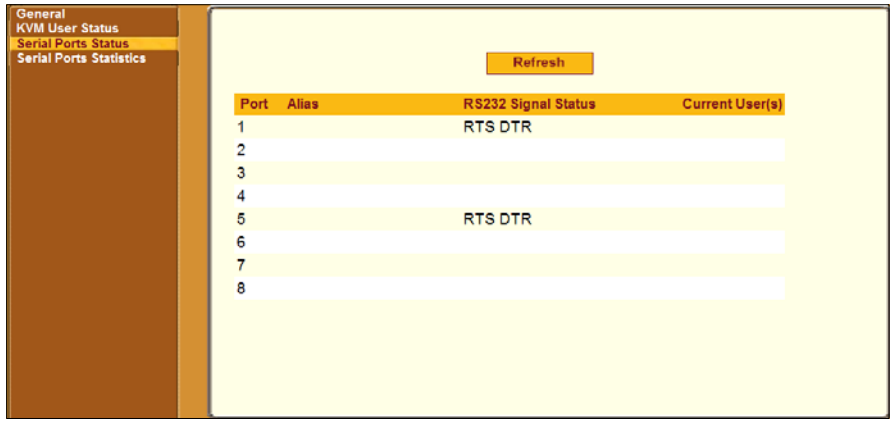


Figure 6-120: Web Manager Information>Serial Port Status Screen

The screen displays status information about serial port connections in the following categories:

- Port Number
- Alias
- RS232 Signal Status
- Current User(s)

▼ *To View Serial Port Status [Expert]*

1. Go to Information>Serial Port in Expert mode.
2. Refresh the display by clicking the “Refresh” button.
3. View the port number, alias, RS232 signal status, and number of current users for all connections to all serial ports.

Information>Serial Ports Statistics

Selecting Information>Serial Port Statistics in Expert mode brings up the screen shown in the following figure.

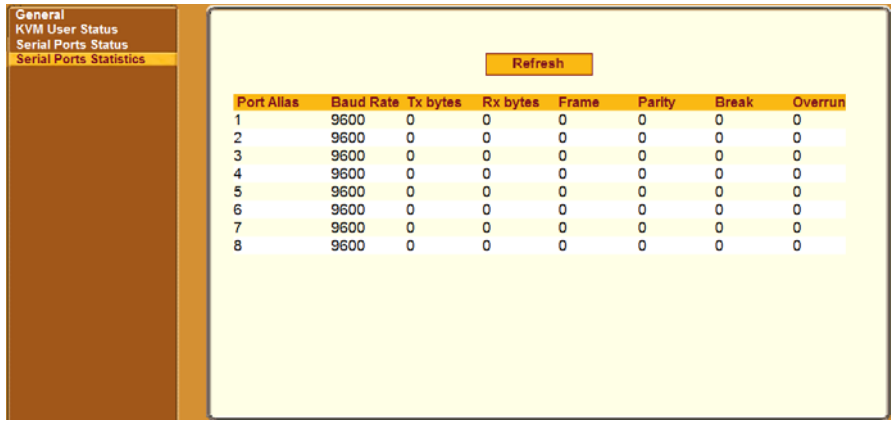


Figure 6-121: Web Manager Information>Serial Port Statistics Screen

An administrative user can use this screen to view serial ports statistics: including baud rate, transfer and response bytes

▼ *To View Serial Port Statistics [Expert]*

1. Go to Information>Serial Port Statistics Expert mode.
2. Refresh the display by clicking the “Refresh” button.
3. View the port alias, baud rate, Tx bytes, Rx bytes, Frame, parity, break, and overrun statistics for all connections to all serial ports.

Management

Under “Management” in Expert mode, six options appear in the left menu, as shown in the following figure.

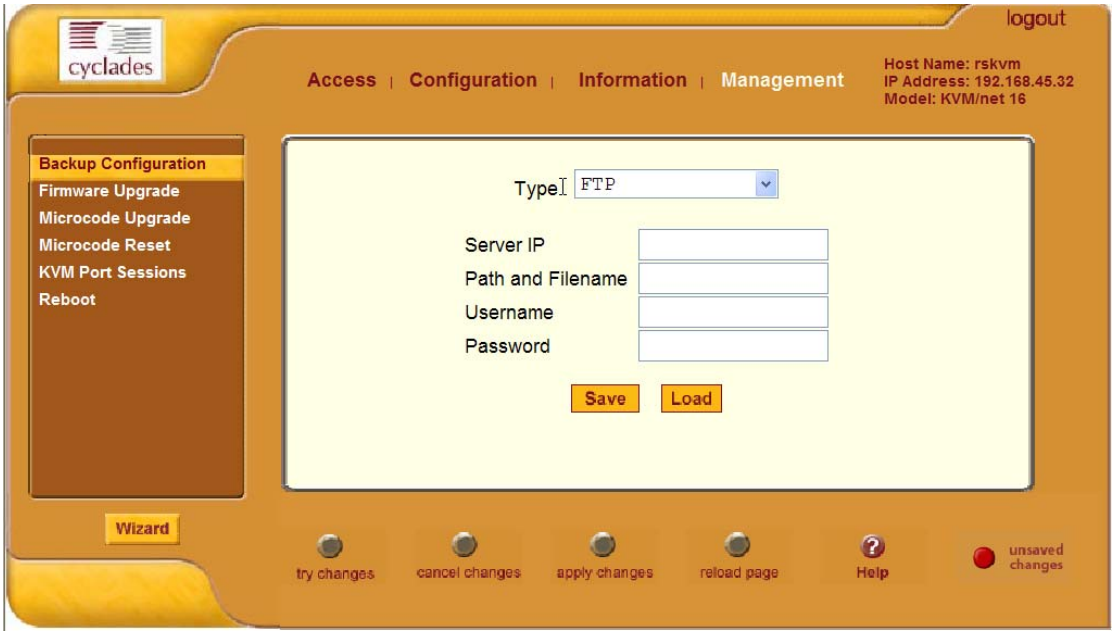


Figure 6-122: Web Manager Management Menu Options

An administrative user can use the Information menu options view various types of information, as described in the following sections.

- “Management>Backup Configuration” on page 364
- “Management>Firmware Upgrade” on page 366
- “Management>Microcode Upgrade” on page 370
- “Management>Microcode Reset” on page 373
- “Management>Reboot” on page 374

An administrative user can use the Management options to do the following:

- Back up the configuration files
- Reboot the OnSite
- Install the following updates

- OnSite firmware (for upgrading the operating system kernel, configuration files, and applications like the Web Manager)
- AlterPath PM IPDU firmware
- KVM Terminator firmware
- Microcode for IP module(s)' microcontroller(s)

Note: Each OnSite has two or three PS2 translation microcontrollers. One microcontroller is for the Local User port. In addition, depending on the number of IP modules, the OnSite has either one or two microcontrollers for KVM over IP users. The microcode update screen lets you update the microcontrollers.

Upgrades are posted for free download at:

- Cyclades's website: `http://cyclades.com`.
- Cyclades's ftp server: `ftp://ftp.cyclades.com`.

Management>Backup Configuration

Selecting Management>Backup Configuration in Expert mode brings up the screen shown in the following figure.

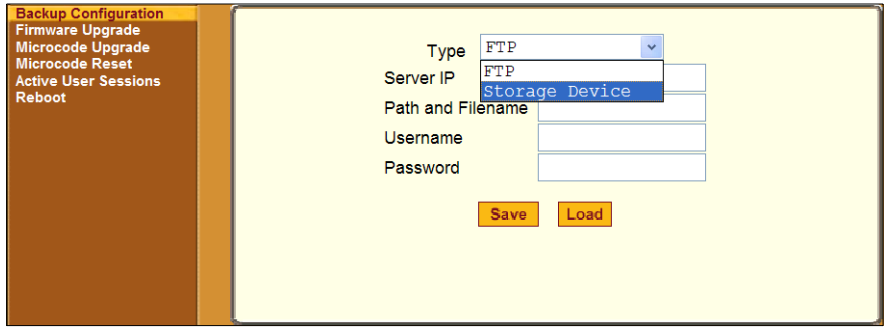


Figure 6-123: Web Manager Management>Backup Configuration Screen

An administrative user can use the "Backup Configuration" screen to backup and restore configuration files. The "Type" pull-down menu options are "FTP" for an ftp server and "Storage Device." The storage device can be either a compact flash or IDE card that was previously inserted in one of the PCMCIA slots, formatted, and configured as described in "Configuration>Network>PCMCIA Management" on page 305.

The “Save” and “Load” buttons appear when either the “FTP” and the “Storage Device” menu options are selected. The “Save” button saves the configuration, and the “Load” restores a previously-saved copy of the configuration files from the selected device.

The previous figure shows the fields that appear when “FTP” is selected from the “Type” pull-down menu. The following table describes the information to enter when FTP is selected.

Table 6-32: Fields on the “Backup Configuration” Screen When FTP is Selected

Field	Definition
Server IP	IP address of an FTP server on the same subnet as the OnSite. (Verify accessibility by pinging the FTP server.)
Path and Filename	Path of a directory on the FTP server where you have write access for saving the backup copy of the configuration file. Specify a filename if you want to save the file under another name. For example, to save the configuration file in a file whose name identifies its origin and date (such as `OnSite8802config040406`) in a directory called “/`upload`” on the FTP server, the following could be entered in the “Path and Filename” field: `/upload/OnSite8802config040406`.
Username and Password	Obtain the username and password to use from the FTP server’s administrator.

When “Storage Device” is selected from the “Type” pull-down menu on the Backup Configuration” screen under “Management” in Expert mode, the “Save” and “Load” buttons appear as shown in the following figure.

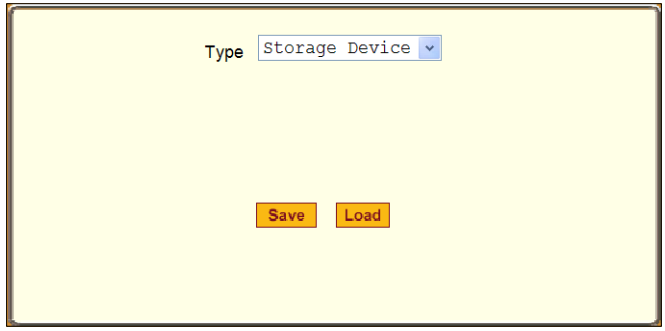


Figure 6-124: Backup Configuration Screen—Storage Device

▼ *To Back Up or Download the OnSite Configuration Files [Expert]*

1. Go to Management>Backup Configuration in Expert mode.

   The Backup Configuration screen appears.

2. Select either “FTP” or “Storage Device” from the “Type” pull-down menu.

3. If you selected “FTP,” do the following steps.

   a. Enter the IP address of the FTP server in the “Server IP” field.

   b. Enter the path of a directory on the FTP server where you have write permissions in the “Path and Filename” field.

   c. Enter a filename after the final slash of the directory path.

4. To backup a copy of the current configuration files, press the “Save” button.

5. To download a previously-saved copy of the configuration files, press the “Load” button.

Management>Firmware Upgrade

Selecting Management>Firmware Upgrade in Expert mode brings up the screen shown in the following figure.

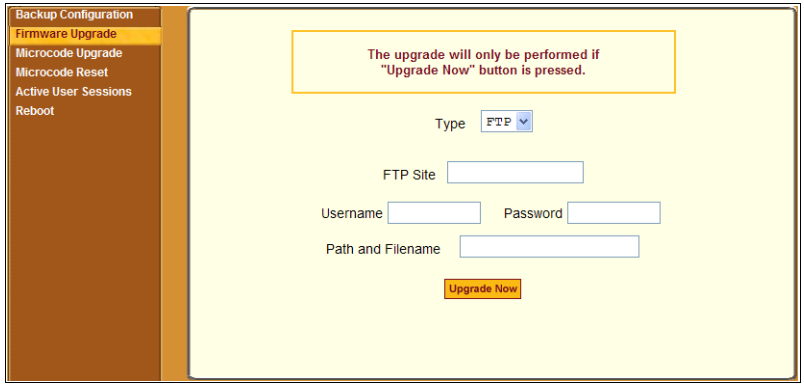


Figure 6-125: Web Manager Management>Firmware Upgrade Screen

An administrative user can use the screen to upgrade the OnSite's operating system kernel, applications, and configuration files, which are collectively referred to as "firmware" in Cyclades management interfaces.

The screen collects information used to automatically download software from an FTP server and to install the software on the OnSite. The following table defines the information you need to supply on the screen.

Table 6-33: Firmware Upgrade Screen Fields and Menu Items

Field/Menu Name	Definition
Type	FTP is the only supported type.
FTP Site	The address of the FTP server where the microcode is located. Any ftp server where the firmware has been downloaded can be used The Cyclades ftp site address is: `ftp.cyclades.com`. If desired, see "To Download AlterPath PM Software From Cyclades [Expert]" on page 200 for how to download the firmware for installation on your own local ftp server.
Username	Username recognized by the `ftp` server. The Cyclades `ftp` username for microcode downloads is "anonymous."
Password	Password associated with the username. An empty password is accepted for anonymous login at the Cyclades ftp server.
Path and File Name	The pathname of the software on the ftp server. On the Cyclades ftp server, the directory is under /`pub/cyclades/alterpath/onsite/released/`*`version_number`*`/filename`, where *`version_number`* is `V_`*`N.N.N.`*, and *`N.N.N`* is the most recent version number, for example, `1.2.1`. The filename includes the version number in the following format: `zImage_ons_`*`NNN`*`.bin`. The pathname for this example would be: `/pub/cyclades/alterpath/onsite/released/V_1.2.0/zImage_ons_121.bin` Go to `ftp://ftp.cyclades.com/pub/cyclades/alterpath/onsite/released` in a browser, if needed, to verify the correct pathname and file names for the software (`zImage`) for the OnSite.

▼ To Find the Cyclades Pathname for Software or Microcode Upgrades [Expert]

Perform this procedure to do the following:

- Find the correct filename for the latest release of the OnSite's operating system kernel, applications, and configuration files, which are collectively referred to as "firmware" in the Cyclades management interfaces.
- Find the correct filename for "microcode" used for other components either used with or within the OnSite, such as the KVM terminators, IP modules, and controllers for IP modules.

1. To find the correct filename for the software or component microcode updates at Cyclades, Corp., enter the following address in a browser:

```
ftp://ftp.cyclades.com/pub/cyclades/alterpath/onsite/released
```

2. In the `released` directory, go to the directory with the latest version number by clicking on the name of the directory.

   For example, if the `released` directory contains directories named `V_1.0.0` and `V_1.1.0`, you would click the `V_1.1.0` directory's name. In the version directory, you would see several files like those shown in the following figure.

   ```
   1.0.6.0-05.09.01.6bin
   KVMswitch_v110.bin
   KVMterm_v112.bin
   zImage_ons_110.bin
   zImage_ons_110.md5
   ```

3. If upgrading the OnSite kernel, applications, and configuration files, take a note of the filename of the file whose name starts with `zImage` and has the `.bin` suffix and go to "To Upgrade the OnSite's Software [Expert]" on page 369.
4. If upgrading the microcode on a KVM terminator, take a note of the filename that starts with `KVMterm` and has the `.bin` suffix and go to "To Download Microcode From an FTP Server [Expert]" on page 372.

5. If upgrading the microcode on microcontrollers that translate PS2 signals, take a note of the filename that starts with `KVMswitch` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server [Expert]” on page 372.
6. If upgrading the microcode for IP modules take a note of the filename that starts with a series of numbers separated by dots, for example, `1.0.6.0-05.09.01.6bin`, and go to “To Download Microcode From an FTP Server [Expert]” on page 372.

▼ *To Upgrade the OnSite’s Software [Expert]*

Perform this procedure to upgrade the latest release of the OnSite’s operating system and applications software, which is referred to as “firmware” in the management interfaces and at the Cyclades website. Upgrading installs the software on the onboard flash memory.

1. In the Web Manager, go to Management >Firmware Upgrade in Expert mode.

   The Firmware Upgrade screen appears.
2. Choose FTP from the Type menu.
3. Enter the name of the ftp server in the “FTP Site” field.

   The Cyclades ftp site address is: `ftp.cyclades.com`.
4. Enter the username recognized by the ftp server in the “Username” field.

   The Cyclades ftp username for firmware downloads is “anonymous.”
5. Enter the password associated with the username on the ftp server in the “Password” field.

   The Cyclades ftp server accepts any password for “anonymous” login.
6. Enter the pathname of the file on the ftp server in the “Path and Filename” field.

   On the Cyclades ftp server, the directory is under `pub/cyclades/alterpath/onsite/released/`*`version_number`*`/`

   See “To Find the Cyclades Pathname for Firmware or Microcode Upgrades” on page 266, if needed.
7. Click the “Upgrade Now” button.

8. Click “cancel changes” (to restore the backed up configuration files).

Management>Microcode Upgrade

Selecting Management>Microcode Upgrade in Expert mode brings up the screen shown in the following figure.

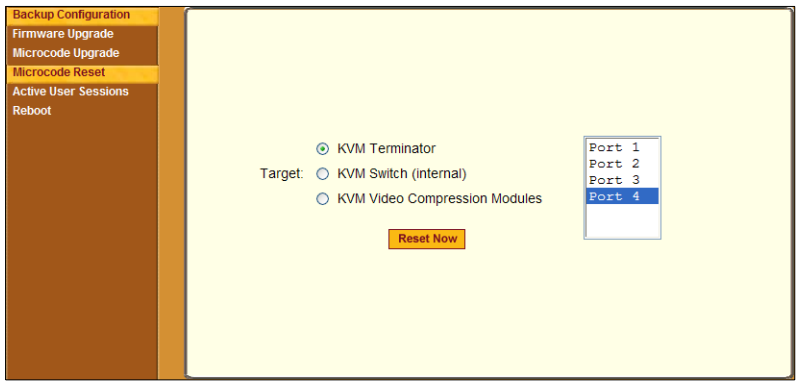


Figure 6-126: Web Manager Management>Microcode Upgrade Screen

As shown in Figure 6-126, if the KVM Terminator radio button is selected, a list of KVM ports appears.

An administrative user can use the Microcode Upgrade screen to specify information used to automatically download microcode from an FTP server and install the microcode on various OnSite components. Either the Cyclades ftp server, `ftp://ftp.cyclades.com`, or a local ftp server where an administrator has previously downloaded the microcode can be used.

Note: Upgrade is not complete until the microcode is reset as described under “To Reset the Microcode After Upgrade [Expert]” on page 373.

The following table shows the terms used on the screen, the corresponding component names, and the filename formats uses for each type of microcode.

Table 6-34: Microcode Filename Formats, Terminology, and Component

Target Name on Screen	Filename Format	Component
KVM Terminator	KVMterm_v*NNN*.bin	All KVM Terminator models

Table 6-34: Microcode Filename Formats, Terminology, and Component (Continued)

Target Name on Screen	Filename Format	Component
KVM Switch (internal)	KVMswitch_v*NNN*.bin	PS2 translation controller for the KVM over IP module (also called the IP module) and for Local User connections
KVM Video Compression Modules	*N.N.N.N-YY.MM.DD.N*.bin	IP module

The actual pathname components must be entered in the "Directory" and "File Name" fields. If needed, go to the following procedure to find the exact name:

- "To Find the Cyclades Pathname for Software or Microcode Upgrades [Expert]" on page 368

The following table defines the information to enter on the screen.

Table 6-35: Microcode Upgrade Field Names and Definitions

Field Name	Definition
Target	The name of the component whose microcode you wish to upgrade (from Table 6-34 on page 370).
FTP Server	The address of the FTP server where the microcode is located. Any ftp server where the firmware is previously downloaded can be specified. The Cyclades ftp site address is: `ftp.cyclades.com`.
Username	Username recognized by the ftp server. The Cyclades ftp username for microcode downloads is "anonymous."
Password	Password associated with the Username. An empty password is accepted for anonymous login at the Cyclades ftp server
Directory	The pathname where the microcode resides on the ftp server. On the Cyclades ftp server, the directory is under /`pub/cyclades/alterpath/onsite/released/`*`version_number`*`/filename`. Go to `ftp://ftp.cyclades.com/pub/cyclades/alterpath/onsite/released` in a browser, if needed, to verify the correct pathname and file names for the microcode for the OnSite.

Table 6-35: Microcode Upgrade Field Names and Definitions (Continued)

Field Name	Definition
File Name	The file name of the microcode for the "Target," as described in Table 6-34 on page 370.

▼ *To Download Microcode From an FTP Server [Expert]*

1. Go to Management>Microcode Upgrade in Expert mode.

   The Microcode screen displays.

2. Click the radio button next to the "Target" whose microcode you want to update.

3. Enter the IP address or name of the ftp server in the "FTP Server" field.

   The Cyclades ftp site address is: `ftp.cyclades.com`.

4. Enter the username recognized by the ftp server in the "User" field.

   The Cyclades ftp username for microcode downloads is "anonymous."

5. Enter the password associated with the username on the ftp server in the "Password" field.

   The Cyclades ftp server accepts an empty password for "anonymous" login.

6. Enter the pathname to the directory where the microcode resides on the ftp server. in the "Directory" field.

   On the Cyclades ftp server, the directory is /`pub/cyclades/alterpath/onsite/`*`released/version_number/`*

7. Enter the name of the microcode file in the "File Name" field.

8. Click the "Upgrade Now" button.

9. Click "apply changes."

10. Go to "To Reset the Microcode After Upgrade [Expert]" on page 272.

Management>Microcode Reset

Selecting Management>Microcode Reset in Expert mode brings up the screen shown in the following figure.

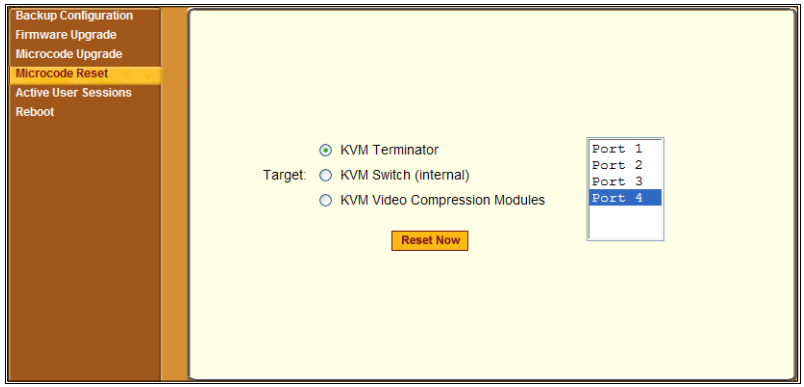


Figure 6-127: Web Manager Management>Microcode Reset Screen

As shown in Figure 6-127, if the KVM Terminator radio button is selected, a list of KVM ports appears.

An administrative user must use this screen to reset the microcode after an upgrade.

▼ *To Reset the Microcode After Upgrade [Expert]*

Perform this procedure if you have upgraded microcode as described in “To Upgrade Firmware [Expert]” on page 267.

1. Go to Management>Microcode Reset.

   The Microcode Reset screen appears.

2. To reset the microcode in a KVM terminator, do the following steps.

   a. Click the KVM Terminator radio button.

      A scrollable list of KVM ports appears.

   b. Select the port to which the KVM terminator is connected.

3. To reset the microcode on a PS2 translation controller, select the radio button next to “KVM Switch (internal).”

4. To reset the microcode on an IP module, select the radio button next to “KVM Video Compression Modules.”
5. Click the “Reset Now” button.

Management>Reboot

Selecting Management>Reboot in Expert mode brings up the Reboot screen shown in the following figure.

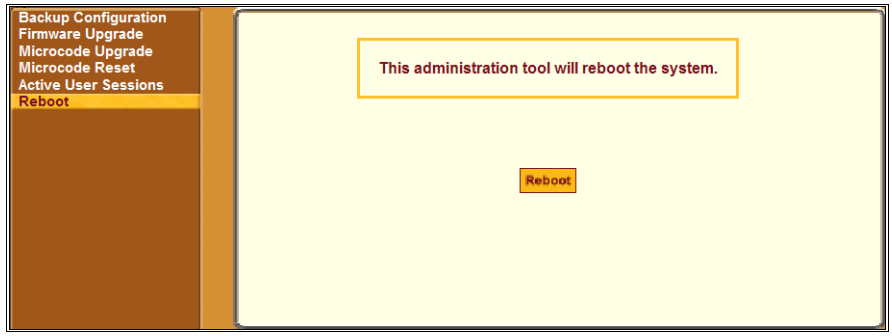


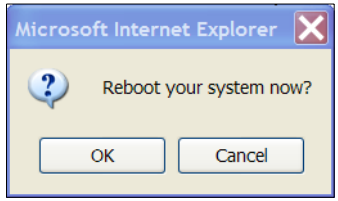
Figure 6-128: Web Manager Management>Reboot Screen

Clicking the “Reboot” button reboots the OnSite.

▼ *To Reboot the OnSite [Expert]*

1. Go to Management>Reboot in Expert mode.
2. Click the Reboot button.

   A confirmation dialog box appears.



3. Click OK.

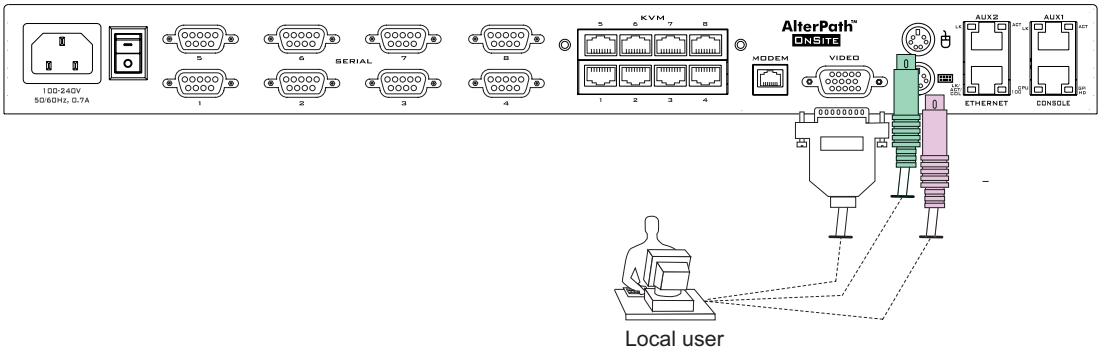
Chapter 7
OSD for All User Types

This chapter describes how to access, navigate, and use the onscreen display (OSD) application.

This chapter covers the topics shown in the following table.

Accessing the OSD

Local OnSite administrators and authorized users can access the OSD through the Local User station, which is a keyboard, monitor, and mouse directly connected to the OnSite. The following figure illustrates a Local User station connected to the keyboard, video and mouse connectors on the back.



The following bulleted items describe rules and restrictions for OSD access.

- OnSite administrative users can access all OSD functions.
- Only one administrative user can access the OnSite at once. Therefore, an administrative user cannot log into the OSD while an administrative user is logged into the Web Manager or the OnSite console.
- The root user cannot access the OSD.
- OnSite administrative users should use the OSD mostly for troubleshooting when a direct connection method is required. OnSite administrative users should perform most configuration tasks through the Web Manager. Similarly, regular users should usually connect to both KVM and serial ports through the Web Manager.
- KVM ports can be accessed through the OSD by administrative users and authorized users.
- Serial ports cannot be accessed through the OSD by either OnSite administrators or authorized users.
- By default, users do not have access to KVM ports. The OnSite administrator must configure the KVM port access permissions before anyone except administrative users can access them.

The following table lists tasks performed using the OSD and provides links to where they are documented.

Table 7-1: OSD Background Information

Related Topic	Where Documented
How OnSite administrators can use the OSD to assign or restrict KVM port access permissions for users	"Configure>Users and Groups Screens [OSD]" on page 450
What you see when you connect to a server through a KVM port (AlterPath Viewer)	"Logging Into the OSD" on page 379
How users use hot keys, share KVM port connections, and common procedures for accessing KVM ports (which are the same whether the ports are accessed using the Web Manager or the OSD)	• "What You See When Connected to a KVM Port" on page 82 • "Sun Keyboard Emulation Hot Keys" on page 87 • "Sharing KVM Port Connections" on page 91 • "Common Procedures for Accessing KVM Ports" on page 93

Logging Into the OSD

The OSD login screen appears when the connected monitor is on.

Figure 7-1: OSD Login Screen

When an OnSite administrator logs in, the Main Menu appears, as shown in the following screen example. (Some of the menu options are not visible.)

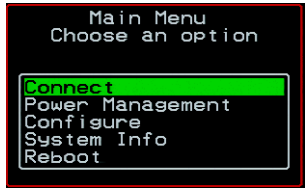


Figure 7-2: OSD Main Menu

See “OSD Main Menu Options for the Administrator” on page 383 for a list of all the Main Menu options and links to where they are documented.

Regular users can access KVM ports through the OnSite. When a regular user logs into the OSD, the Connection Menu appears. The Connection Menu lists the KVM ports the user is authorized to access by their default port names or administrator-defined aliases, as shown in the following screen example.

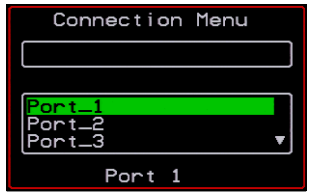


Figure 7-3: OSD Connection Menu

The Connection Menu includes the Exit option, and it also includes the Cycle option if the logged in user has permission to access two or more ports, as shown in the following screen example.

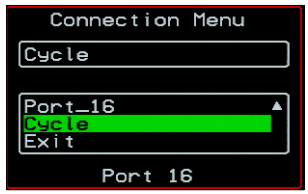


Figure 7-4: OSD Connection Menu With Cycle and Exit Options

See “Connection Menu” on page 89 for more details.

▼ *To Log Into the OSD*

1. Turn on the monitor that is connected to the Local User port on the OnSite.
2. Enter the Login name.
3. Enter the Password.

   If you are logging in as an administrative user, the OSD Main Menu appears. See “OSD Main Menu Options for the Administrator” on page 383 for links to administrative procedures.

   If you are logging in as a regular user authorized to access KVM ports, the Connection Menu appears. See “To Log Into a Server Connected to a KVM Port” on page 94.

Navigating the OSD

Users can use *navigation keys* to move between the OSD screens and to make menu selections as described in the following sections:

- “Basic OSD Navigation Keys” on page 381
- “Common OSD Navigation Actions” on page 382

Note: The escape (Esc) key can be used at any point to exit from the current screen. For example, if a user is connected to a port, the user can enter the Esc key to return to the Connection Menu, enter Esc again to return to the Main Menu, and then enter Esc again to return to the OSD login screen.

Basic OSD Navigation Keys

Users can use the keys listed in following table to navigate the OSD.

Table 7-2: Basic OSD Navigation Keys

Key	Action
Up ↑ Down ↓	Move up and down among menu options.
Page Up / Page Down	Skip up or down three lines in a menu.
Home	Move to the top of a menu
End	Move to the end of a menu
Tab	Change between fields on a screen.
Backspace	Delete character left to the cursor.
Left ⇠ Right ⇢	Select a button at the bottom of the screen
Enter	Select highlighted item; Commit changes

Common OSD Navigation Actions

The “Action” column in Table 7-3 shows wording used to refer to common actions performed while working in the OSD. The “OSD Equivalent” column describes the keys to use in the OSD screens to perform the actions.

Table 7-3: Performing Common OSD Navigation Actions

Action	OSD Equivalent
Select *button_name*	Tab or use one of the arrow keys to get to the button and press “Enter.”
Save changes	Tab or use one of the arrow keys to get to the Save button and press “Enter.”
Select an option	Tab or use one of the arrow keys to get to the option and press “Enter.”
Go to a specific screen, as in: “Go to Configure>Users and Groups.”	Select the first option from the Main menu. On the next screen that comes up select the next option from that menu. Do this until you get to the last option in the menu path.

Power Management Through the OSD

See “Power Management” on page 50 for an overview of how power is managed on the OnSite, if needed.

The following two types of power management can be done through the OSD.

- IPDU power management
- Power management of servers while connected to KVM ports

IPDU Power Management (OSD)

Only administrative users can use the OSD to perform power management of outlets on connected and configured AlterPath PMs. See “Power Management Menu [OSD]” on page 384 and other sections referenced there for the Power Management screens available to administrative users and for how to use them.

Power Management While Connected to a KVM Port (OSD)

Both administrative users and authorized users can perform power management while connected to a KVM port.

Power management while connected is the same whether the KVM port connection was made through the OSD or the Web Manager. See “Power Management” on page 76 for the prerequisites that must be complete before anyone can perform power management while connected and for the procedures.

OSD Fan Failure Warning

If one of the OnSite’s fan’s is stopped, a beep sounds, and the OSD displays a warning. Click enter to confirm the warning message has been received.

OSD Main Menu Options for the Administrator

Table 7-4 gives a brief description of each option on the Main Menu and lists where OnSite administrators can find more information.

Table 7-4: OSD Main Menu Options

Menu Selection	Purpose	Where Documented
Connect	Connect to a KVM port.	“To Log Into a Server Connected to a KVM Port” on page 94
Power Management	View status of all outlets on connected IPDUs and power on, power off, and cycle the outlets.	“Power Management Menu [OSD]” on page 384
Configure	View the Configuration Menu and select options for configuring the OnSite, users, and ports.	“Configure Menu Overview [OSD]” on page 386
System Info	View system information.	“System Info Menu [OSD]” on page 497

Table 7-4: OSD Main Menu Options

Menu Selection	Purpose	Where Documented
Reboot	Reboot the OnSite.	“Reboot [OSD]” on page 499

Power Management Menu [OSD]

Choosing “Power Management” from the OSD Main menu brings up the Power Management screen as shown in the following figure.

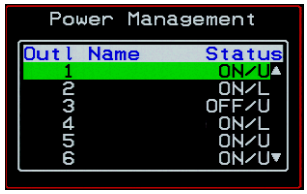


Figure 7-5: OSD Power Management Screen

The screen displays a list of all outlets on all AlterPath PM IPDUs connected to the OnSite. See “Power Management” on page 50 for an introduction to power management on the OnSite, if needed.

The Status column displays whether the outlet is on (ON), off (OFF), locked (L), or unlocked (U).

Note: To quit the power management menu or any of the related screens, press Esc.

When the administrative user select an outlet, the “Outlet Status” screen appears as shown in the following figures. The “Status” box in the middle of the screen displays the current status for the selected outlet and buttons appear on the bottom of the screen to allow you to change the outlet’s status.

When an outlet is on and unlocked, “Off,” “Lock,” and “Cycle” buttons appear, as in the following figure.

Figure 7-6: Outlet Status Screen—Outlet Unlocked

When an outlet is off and unlocked, the “On,” “Lock,” and “Cycle” options appear, as in the following figure.

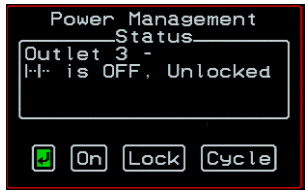


Figure 7-7: Outlet Status Screen—Outlet Off and Unlocked

When an outlet is on and locked, only the “Unlock” option appears, as shown in the following figure.

To Power On, Power Off, Lock, Unlock, or Cycle Power Outlets [OSD]

Follow this procedure to manage power outlets on connected and configured IPDUs. See“Power Management” on page 50 for background information, if needed.

1. Log into the OSD.

   See “To Log Into the OSD” on page 380 if needed.

2. Go to Configure>Power Management.

3. Select the outlet to edit.

4. Select On, Off, Lock, Unlock, or Cycle as appropriate.
5. To change the status of other outlets, repeat steps 2 and 3.
6. Hit Esc until you get to the next menu you want to access.

Configure Menu Overview [OSD]

An administrative user can select “Configure” from the OSD Main Menu brings up the Configuration Menu. The Configuration Menu provides a number of options, as shown in the following screen.

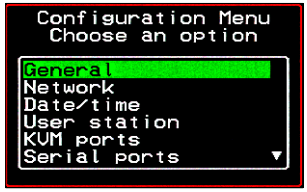


Figure 7-8: Configure Menu Options

Not all the configuration menu options are visible in Figure 7-8. Table 7-5 gives a brief description of all the OSD configuration menu options and provides links to where the features are documented.

Table 7-5: OSD Configuration Menu Options (Sheet 1 of 3)

Menu Selection	Purpose	Where Documented
General	Configure authentication type for direct logins to KVM ports; syslog facility number; KVM connection hot key escape sequence, and Sun Keyboard emulation hot key escape sequence. **Note:** syslogging also requires configuration of the syslog server using the Syslog option, described later in this table.	“Configure>General Screens [OSD]” on page 389
Network	Configure DHCP or assign an IP address and configure other basic network parameters; configure SNMP, VPN, IP filtering, hosts, and static routes	“Configure>Network> Network Screens [OSD]” on page 397

Table 7-5: OSD Configuration Menu Options (Sheet 2 of 3)

Menu Selection	Purpose	Where Documented
Date/Time	Enable/disable NTP or manually configure the system date and time.	"Configure>Network> Date/time Screens [OSD]" on page 426
User station	Configure the Local User station's idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current workstation.	"Configure>User Station Screens [OSD]" on page 427
KVM ports	Activate KVM ports, assign aliases, and enable power management.	"Configure>KVM Ports Screens [OSD]" on page 436
Serial ports	Activate serial ports, assign aliases, enable power management, set the baud rate, access permissions, and an authentication method for one or more ports.	"Configure>Serial Ports Screens [OSD]" on page 440
Users and groups	Configure users and groups, user passwords, and KVM port access permissions.	"Configure>Users and Groups Screens [OSD]" on page 450
Syslog	Configure the IP address of the syslog server. **Note:** syslogging also requires assignment of a facility number using the General option, described earlier in this table.	"Configure>Syslog Screens [OSD]" on page 466
PCMCIA	Configure PCMCIA cards.	"Configure>PCMCIA Screens [OSD]" on page 466
Authentication	Configure an authentication method for OnSite logins and authentication servers for OnSite, KVM, and serial port logins.	"Configure>Authentication Screens [OSD]" on page 470

Table 7-5: OSD Configuration Menu Options (Sheet 3 of 3)

Menu Selection	Purpose	Where Documented
Save/Load Config	Permanently save configuration changes, load stored a configuration or restore the configuration to factory default values.	"Configure>Date/Time [OSD]" on page 480
Exit	Exit from the menu.	N/A

Understanding OSD Configure Screen Series

Selecting an option from the "Configure" menu usually brings up to a series of related screens, which the administrative user navigates through one at a time until the final screen is reached.

For example, if Date/Time is selected, a series of "Date/time Config." screens appears starting with "NTP" and ending with "Time," as shown in the following figure.

Figure 7-9: Example Screens in Configure Screen Series

As illustrated, all configuration screens except the final one have a right arrow at the bottom right that an administrative user can click to go to the next screen. Clicking "Save" on any of the screens saves any changes made to that point. An administrative user can also wait for the final screen in a series before saving changes. Clicking "Save" on the final screen saves any change and returns to the Configuration menu.

Note: The Save button on every screen saves configuration changes into the configuration files. To permanently back up all configuration changes so they can be restored after an upgrade, you must also select “Save/Load Conf.” from the Configuration Menu. See “How Configuration Files Changes Are Managed” on page 574 for more details.

See “Navigating the OSD” on page 381, if needed, for how to use the Tab key and other keys to move around the screens in the OSD.

Configure>General Screens [OSD]

An administrative user can select the General option on the OSD Configure Menu to configure several general features of the OnSite.

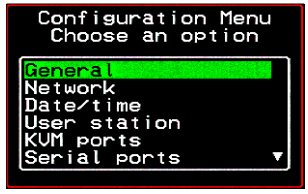


Figure 7-10: Selecting OSD Configure>General

Selecting Configure>General from the OSD Main Menu brings up the Authentication type screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-6 gives a brief description of the sequence of General configuration screens.

Table 7-6: Configure>General Screens [OSD] (Sheet 1 of 2)

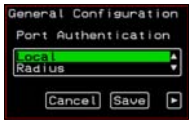
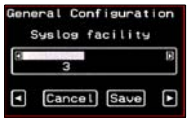
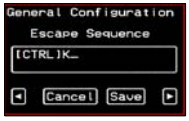
Screen	Description
Authentication Type 	The authentication type that applies to *direct KVM port logins from the Web Manager login screen*: None, Local, Radius, TacacsPlus, Kerberos, LDAP, RadiusDownLocal, TacplusDownLocal, KerberosDownLocal, LdapDownLocal, NTLM(Win NT/2k/2k3), and NTLMDownLocal. Direct logins to KVM ports must also be enabled. (See “Direct Access” on page 391.) You also must ensure that an authentication server is specified for the type of method you select. See “Configure>Authentication Screens [OSD]” on page 470.
Syslog Facility 	The syslog facility number that is used by the administrator of the syslog server to identify messages generated by devices connected to the KVM ports. Obtain the facility number to use for the OnSite from the syslog server’s administrator. Values are from 0 through 7. See “Syslog Servers” on page 28 for examples of using facility numbers as needed. In addition, the IP address of the syslog server must be configured, as described under “Configure>Syslog Screens [OSD]” on page 466.
Escape Sequence 	The escape sequence for KVM port connection hot keys. The default is `Ctrl+k`, shown as `[CTRL]K` in the screen. Enter the keys in all caps. The format and valid escape sequence modifier keys are [CTRL], [SHIFT[, [ALT], and [WIN], the Windows key with the Windows logo on it. See “Configuring KVM Port Connection Hot Keys” on page 63 for more details.
Sun Keyboard 	The escape key for Sun hot keys. Default: [WIN]. Other options are: [CTRL], [SHIFT], and [ALT]. See “Sun Keyboard Emulation Hot Keys” on page 87 and “Configuring Sun Keyboard Equivalent Hot Keys” on page 64 for more details.

Table 7-6: Configure>General Screens [OSD] (Sheet 2 of 2)

Screen	Description
IP Security Level 	The level of encryption: “None,” “Kbd/Mouse”—encrypt keyboard and mouse data,” or “Video/Kbd/Mouse”—encrypt data from the keyboard, video, and mouse.
DES 	Selecting “Yes” enables and “No” disables 3DES encryption.
Direct Access 	Selecting “Yes” enables and “No” disables direct access to KVM ports from the Web Manager login screen.
TCP Port Viewer 	Allows you to assign an alternate TCP Port number or numbers for the AlterPath Viewer to use [Default, 5900+]. Use the plus sign (+) to increment the port number by 1 for each additional AlterPath Viewer. You might need to assign another port, for example, if your Internet provider is blocking port 5900. For example: 5903+ means that the first AlterPath Viewer uses port 5903 and the second uses port 5904. Use the hyphen (-) to indicate a range of addresses, for example, 5903-5907. Use the comma (,) to separate two TCP port addresses, for example, 5901,5903. Combine commas and hyphens, as desired, for example: 1901,5903-5905,5907. **Note:** Do not use reserved port numbers 1 through 1024.

Configure>General: Authentication Type Screen

An administrative user can use the “Authentication type” screen under Configure>General in the OSD to configure an authentication type for direct logins to KVM ports. An authentication server must be available and

configured for the selected type of method. See “OnSite Authentication Options” on page 7 for an overview of authentication on the OnSite, if needed.

▼ *To Configure an Authentication Type for Direct KVM Port Access*

1. Go to: Configure>General>Authentication Type.

   The Authentication type screen appears.

2. On the Authentication Type screen, select an authentication type.

   See “OnSite Authentication Options” on page 7 for background information on choosing the appropriate authentication method.

3. Save the changes.

Configure>General: Syslog Facility Screen

The facility number entered on this screen is used by the administrator of the syslog server to identify messages generated by devices connected to the KVM ports. “Syslog Servers” on page 28 gives examples of using facility numbers.

▼ *To Configure a Syslog Facility Number [OSD]*

Obtain the facility number to use for the OnSite from the system administrator of the syslog server.

1. Go to: Configure>General>Authentication Type>Syslog Facility.

   The “Syslog Facility” screen appears.

2. Enter the value (0 through 7) that the administrator of the syslog server has assigned.

3. Save the changes.

Configure>General: Escape Sequence Screen

By default, the AlterPath Viewer escape sequence (the first portion of all AlterPath Viewer hot keys) is Ctrl+k. On the Escape Sequence screen, you

can change the first portion of the hot keys. See “Configuring Keyboard Shortcuts (Hot Keys)” on page 63 for more details.

▼ *To Define the Escape Sequence for AlterPath Viewer Hot Keys [OSD]*

1. Go to: Configure>General>Authentication Type>Syslog Facility>Escape Sequence.

   The “Escape sequence” screen appears.

2. Enter the key sequence to be used as the first portion of all AlterPath Viewer hot keys.

Configure>General: Sun Keyboard Screen

You can use the Sun Keyboard screen to substitute an alternative escape key for Sun keyboard emulation hot keys. The default is [WIN]

▼ *To Configure Emulation of a Sun Keyboard [OSD]*

1. Go to: Configure>General>Authentication Type>Syslog Facility>Escape Sequence> Sun Keyboard.

   The “Sun Keyboard” screen appears.

2. On the Sun Keyboard screen, enter an alternative Sun emulation hot key escape key [Default: WIN].

3. Save the changes.

Configure>General: IP Security Level Screen

You can use the IP Security Level screen to select the level of IP security to include keyboard and mouse, OR keyboard, video and mouse, OR none.

▼ *To Configure the IP Security Level [OSD]*

1. Go to: Configure>General>Authentication Type>Syslog Facility>Escape Sequence>Sun Keyboard>IP Security Level.

   The “IP Security” screen appears.

2. On the IP Security screen, select the IP security level (None, Keyboard/Mouse, or Keyboard/Video/Mouse).
3. Save the changes.

Configure>General: 3DES Screen

You can use the 3DES OSD screen to configure 3DES encryption for communications between the OnSite and the remote user connected to a KVM port. The default is RC4.

▼ *To Enable or Disable 3DES Encryption* [OSD]

1. Go to: Configure>General>Authentication Type>Syslog Facility> Escape Sequence>Sun Keyboard>IP Security Level >3DES.

   The “enable 3DES” screen appears.
2. Select Yes or No.
3. Save the changes.

Configure>General: Direct Access Screen

Enabling Direct Access allows users to access a KVM port directly from the Login screen of the Web Manager by entering the name or alias for the port in a Port field.

▼ *To Enable Direct Access to KVM Ports* [OSD]

1. Go to: Configure>General>Authentication Type>Syslog Facility> Escape Sequence>Sun Keyboard>IP Security Level >3DES>Direct Access.

   The “Direct Access” screen appears.
2. Select Yes or No.
3. Save the changes.

Configure>General: TCP Viewer Port Screen

An administrative user can use the TCP Viewer Port screen to assign an alternate TCP port or range of ports for the AlterPath Viewer to use instead of the default, 5900+.

Note: Do not use reserved port numbers 1 through 1024.

▼ *To Assign Alternate TCP Port Numbers for the AlterPath Viewer* [OSD]

1. Go to: Configure>General>Authentication Type>Syslog Facility> Escape Sequence>Sun Keyboard>IP Security Level >3DES>Direct Access>TCP Viewer Port.

   The “TCP Port” screen appears.

2. Type in the desired TCP Port for the AlterPath Viewer to use, making use of the following conventions:

   - Use the plus sign (+) after a TCP port number to increment the port number by 1 for each additional AlterPath Viewer that is launched. For example: 5903+ means that the first AlterPath Viewer uses port 5903 and the second uses port 5904.
   - Use the hyphen (-) to indicate a range of addresses. For example, 5903-5907.
   - Use the comma (,) to separate two TCP port addresses. For example, 5901,5903.
   - Combine commas and hyphens, as necessary For example, 1901,5903-5905,5907

3. Select Save to complete the General Configuration.

Configure>Network Menu Options [OSD]

An administrative user can select the Network option on the Configuration Menu to configure network-related services for the OnSite.

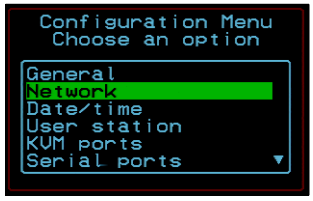


Figure 7-11: Selecting OSD Configure>Network

Selecting Network brings up the Network Configuration Menu. The Network Configuration Menu provides a number of options, as shown in the following screen.

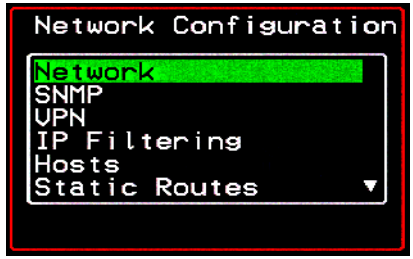


Figure 7-12: OSD Networking Configuration Menu

Not all the options are visible. The following diagram lists the names of all the configuration options accessed from the Configure>Network menu.

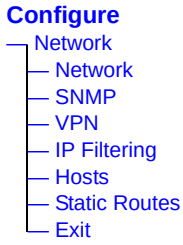


Figure 7-13: OSD Configure>Network Menu Options

The configuration screen series for each of the options under Configure>Network are listed and described in the following sections:

Configure>Network>Network Screens [OSD]

An administrative user can select the Network option from the Network Configuration menu to configure DHCP or configure a fixed IP address and other basic network parameters.

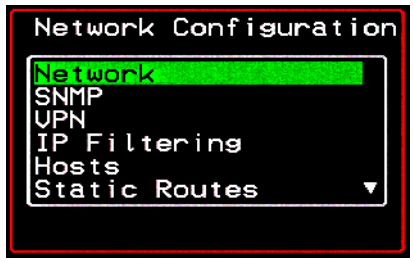


Figure 7-14: Selecting Network From the OSD Network Configuration Menu

The following diagram lists the names of the series of configuration screens accessed under Configure>Network>Network.

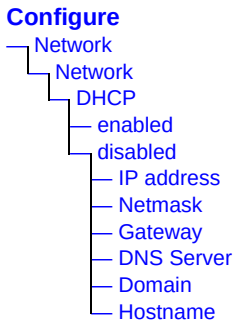


Figure 7-15: OSD Configure>Network>Network Screens

Selecting Configure>Network>Network from the OSD Main Menu brings up the DHCP screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-7 gives a description of all the related configuration screens.

Table 7-7: Network Configuration Screens [OSD] (Sheet 1 of 2)

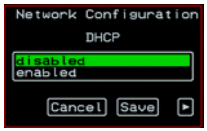
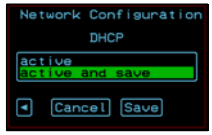
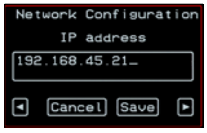
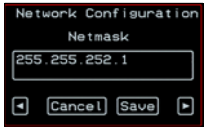
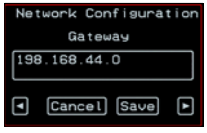
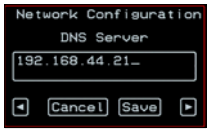
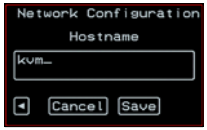
Screen	Description
DHCP 	Enable or disable DHCP. When you select “enabled,” the screen shown in the following figure appears.  “active” saves the changes to the configuration files. “active and save” overwrites the backup configuration files and makes the changes permanent. Either choice brings you back to the Network Configuration menu. When “disabled” is selected, the IP address, Netmask, Gateway, DNS Server, Domain, and Hostname screens appear in the sequence shown in the following rows.
IP Address 	The IP address of the OnSite.
Netmask 	The netmask for the subnet (if applicable) in the form *NNN.NNN.NNN.N* (for example: `255.255.252.0`).
Gateway 	The IP address for the gateway (if applicable).

Table 7-7: Network Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
DNS Server 	The IP address for the DNS server.
Domain 	The domain name.
Hostname 	The hostname for the OnSite.

▼ *To Configure Basic Networking [OSD]*

1. From the OSD Main Menu, go to Configure>Network.

   The Network Menu appears.

2. From the Network Menu, select Network again.

   The DHCP screen appears.

3. To enable DHCP, do the following steps.

   a. Select the “enabled” option.

   b. Press Enter.

      The next DHCP screen appears.

   c. Select “enable” or “enable and save.”

4. To enter network parameters manually, do the following steps.

   a. Select the “disabled” option.

b. Press Enter.

The IP address screen appears.

c. Enter the IP address for the OnSite and go to the next screen.

The Netmask screen appears.

d. Enter the netmask (in the form 255.255.255.0) and go to the next screen.

The Gateway screen appears.

e. Enter the IP address for the gateway and go to the next screen.

The DNS Server screen appears.

f. Enter the IP address for the DNS server and go to the next screen.

The Domain screen appears.

g. Enter the domain name and go to the next screen.

The Hostname screen appears.

h. Enter the hostname for the OnSite and save the changes to complete the basic network configuration.

Configure>Network>SNMP Screens [OSD]

An administrative user can select the SNMP option from the Network Configuration menu to configure SNMP.

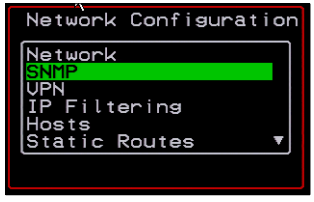


Figure 7-16: Selecting SNMP From the OSD Network Configuration Menu

The following diagram lists the names of the configuration screens accessed under Configure>Network>SNMP.

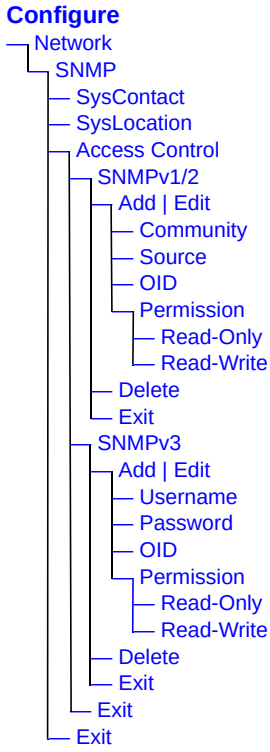


Figure 7-17: OSD Configure>Network>SNMP Screens

See “SNMP on the OnSite” on page 53 for details.

Table 7-8 gives a brief description of all the SNMP configuration screens.

Table 7-8: SNMP Configuration Screens [OSD] (Sheet 1 of 3)

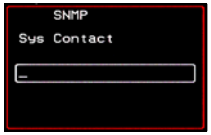
Screen	Description
SysContact 	The email address for the OnSite’s administrator, for example: `onsite_admin@cyclades.com`.

Table 7-8: SNMP Configuration Screens [OSD] (Sheet 2 of 3)

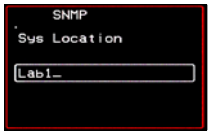
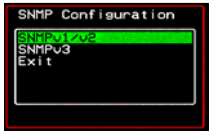
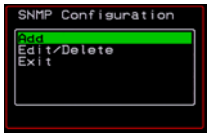
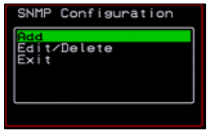
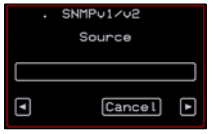
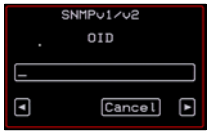
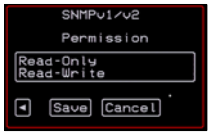
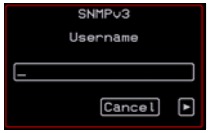
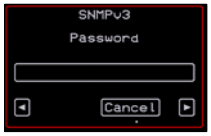
Screen	Description
SysLocation 	The physical location of the OnSite.
Access Control 	Choices are SNMP v1/2 or SNMP v3.
SNMP Configuration 	Appears when either SNMP v1/2 or SNMP v3 is selected. Choices are “Add,” “Edit/Delete,” or “Exit.”
SNMPv1/v2 Community 	The community name is sent in every SNMP communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under “Permission”: either read only or read write. The most common community is “public” and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the OnSite.
SNMPv1/v2 Source 	The source IP address. Accepted values are “default” or a subnet address, for example: `193.168.33.0/24`.

Table 7-8: SNMP Configuration Screens [OSD] (Sheet 3 of 3)

Screen	Description
SNMPv1/v2 or v3 OID 	Object Identifier. Each managed object has a unique identifier.
SNMPv1/v2 or v3 Permission 	Choices are “Read-Only” and “Read-Write.” Read Only - Read-only access to the entire MIB (Management Information Base) except for SNMP configuration objects. Read/Write - Read-write access to the entire MIB except for SNMP configuration objects.
SNMPv3 Username 	User name.
SNMPv3 Password 	Password.

Configure>Network>VPN Screens [OSD]

An administrative user can select the VPN option from the Network Configuration menu to add a VPN connection or to edit or delete a previously-

configured VPN connection. See “VPN on the OnSite” on page 54 for additional details.

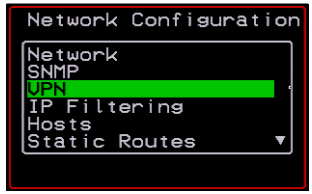


Figure 7-18: Selecting VPN from the Network Configuration Menu

Selecting VPN under Configuration>Network brings up the VPN Configuration Menu. The VPN Configuration Menu provides the options shown in the following screen.

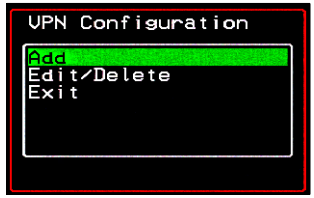


Figure 7-19: OSD Configure>Network>VPN Configuration Menu

The following diagram lists the names of the configuration screens accessed from the Add and Edit/Delete options on the Configure>Network>VPN Configuration menu.

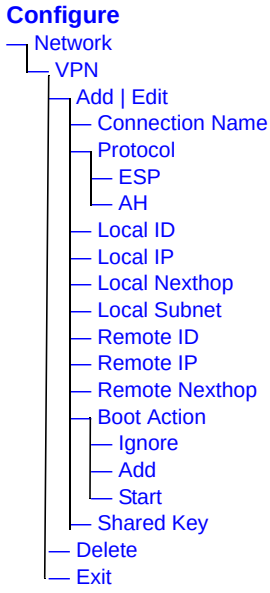


Figure 7-20: OSD Configure>Network>VPN Options and Screens

Table 7-9 gives a brief description of the VPN configuration screens series under Add and Edit.

Table 7-9: VPN Configuration Screens [OSD] (Sheet 1 of 3)

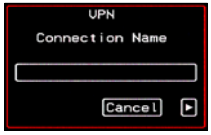
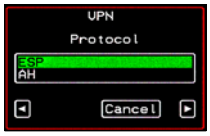
Screen	Description
Connection Name 	Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN.”
Protocol 	The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header).

Table 7-9: VPN Configuration Screens [OSD] (Sheet 2 of 3)

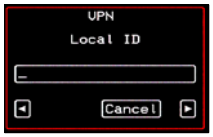
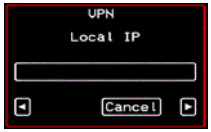
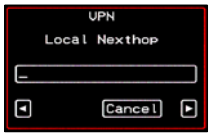
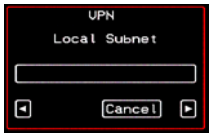
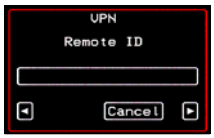
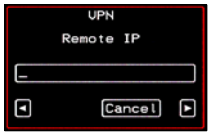
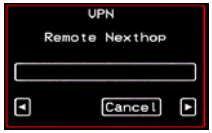
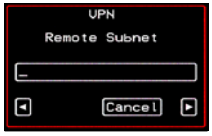
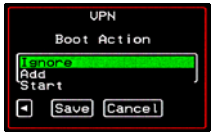
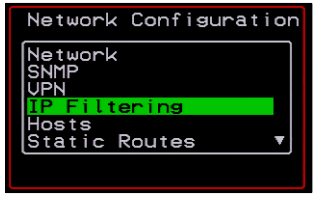
Screen	Description
Local ID 	The hostname of the OnSite, referred to as the “local” host.
Local IP 	The IP address of the OnSite.
Local NextHop 	The router through which the OnSite sends packets to the host on the other side.
Local Subnet 	The netmask of the subnetwork where the OnSite resides, if applicable.
Remote ID 	The hostname of the remote host or security gateway

Table 7-9: VPN Configuration Screens [OSD] (Sheet 3 of 3)

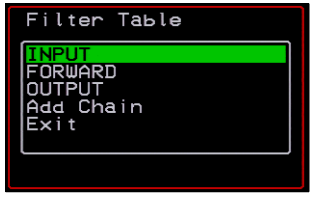
Screen	Description
Remote IP 	The IP address of the remote host or security gateway.
Remote Nexthop 	The IP address of the router through which the host on the other side sends packets to the OnSite.
Remote Subnet 	The netmask of the subnetwork where the remote host or security gateway resides, if applicable.
Boot Action 	Choices are “Ignore,” “Add,” and “Start.” “Ignore” means that VPN connection is ignored. “Add” means to wait for connections at startup. “Start” means to make the connection.
Shared Key 	Pre-shared password between left and right users.

Configure>Network>IP Filtering Screens [OSD]

An administrative user can select the IP Filtering option from the Network Configuration menu to configure the OnSite to filter packets like a firewall. See “Packet Filtering on the OnSite” on page 65 for details.



Selecting IP Filtering under Configure>Network brings up the “Filter Table.” The “Filter Table” lists the default chains along with any administratively-configured chains, the “Add Chain,” and the “Exit” options, as shown in the following screen.



An administrative user can use this menu to create chains and set up rules for the new chains, or to edit or delete a previously-configured chain. The following diagram lists the names of the configuration screens accessed under Configure> Network>IP Filtering.

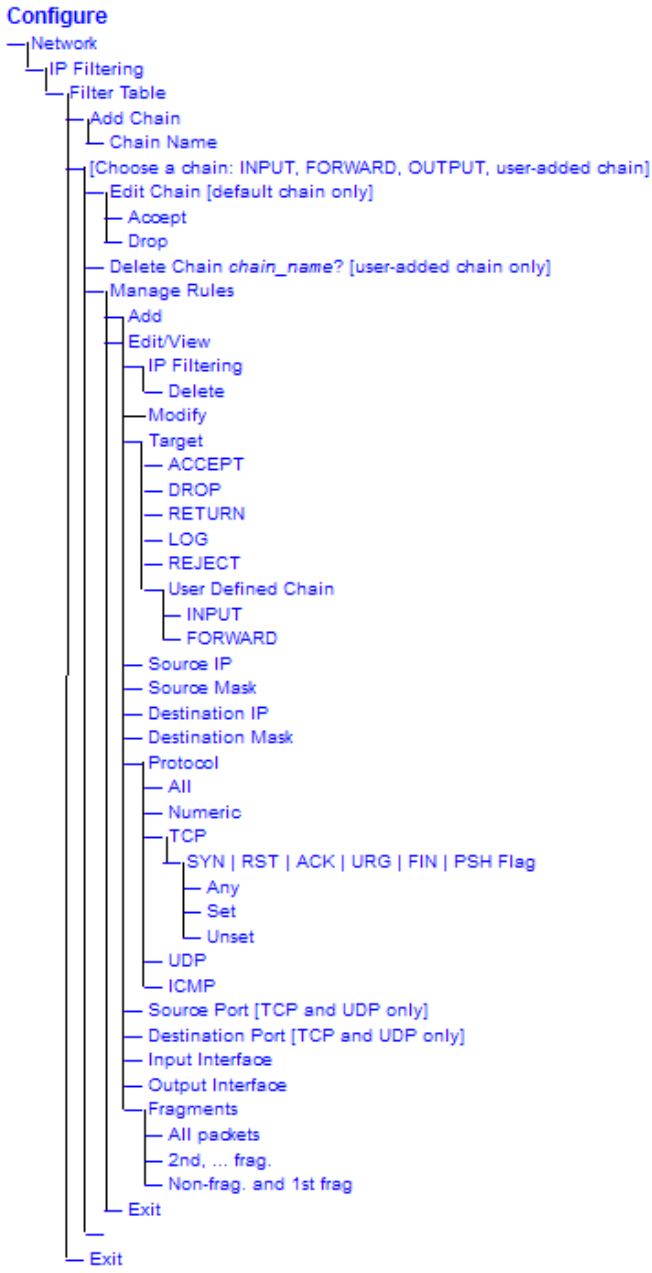


Figure 7-21: OSD Configure>Network>IP Filtering Screens

The following table shows the IP filtering screens.

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 1 of 6)

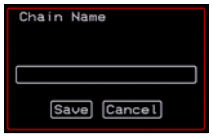
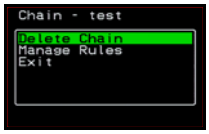
Screen	Description
Filter Table 	Lists the default chains along with any administratively-configured chains, the “Add Chain,” and the “Exit” options.
Chain Name 	Only appears when “Add Chain” is selected. Entering the name of the chain adds the new chain’s name to the “Filter Table,” where you need to select the name of the new chain and define rules for the chain.
Chain - *chain_name* options 	Appears when a user-added chain is selected from the “Filter Table.” The choices are “Delete Chain,” “Manage Rules,” “Exit.”
Delete Chain *chain_name?* 	Appears when a user-added chain is selected and the “Delete Chain” option is chosen from the “Chain - *chain_name*” menu.
Chain - *CHAIN_NAME* 	Appears when a default chain is selected from the “Filter Table.” The choices are “Edit Chain,” “Manage Rules,” and “Exit.”

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 2 of 6)

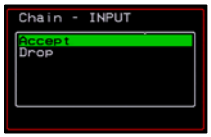
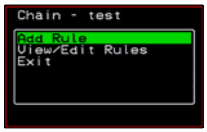
Screen	Description
Chain - *CHAIN_NAME* Edit options 	Appears when a default chain is selected and the “Edit Chain” option is chosen from the Chain - *Chain_name* menu. Defines the default action to take on packets of this type. Choices are “Accept” or “Drop.”
Chain - *chain_name* “Manage Rules” options 	Appears when a user-defined chain is selected and the “Manage Rules” option is selected from the Chain-*chain_name* menu. Choices are “Add Rule,” “View/Edit Rules” or “Exit.” The packet is filtered for the characteristics defined for the rule in the following screens, for example, a specific IP header, input and output interfaces, TCP flags or protocol. The target action is performed on all packets that have the characteristic. If “Inverted” is selected for a characteristic, the target action is performed on all packets that do not have the characteristic.
IP Filtering 	Appears when “View/Edit Rules” is selected from the “Manage Rules” menu. All the characteristics are listed in the menu. “Modify” and “Delete” buttons are at the bottom of the screen.
Target 	Appears when a user-added chain is selected along with “Add Rule” or “View/Edit Rules.” Choices specify the target action to take when a packet’s characteristics match the rule, or, if “Inverted” is selected, if the packets do not match the rule. Choices are: “ACCEPT,” “DROP,” “RETURN,” “LOG,” “REJECT,” and “User Defined Chain.”

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 3 of 6)

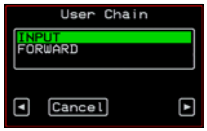
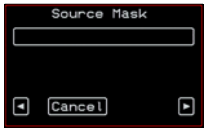
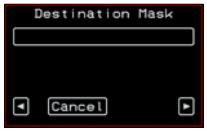
Screen	Description
User Chain 	Appears when “User Defined Chain” is selected from the “Target” menu. Choices are: “INPUT,” and “FORWARD.”
Source IP 	The IP address of the source of an input packet.
Source Mask 	The netmask of the subnetwork where an input packet originates.
Destination IP 	The IP address of an output packet’s destination.
Destination Mask 	The netmask of the subnet to which an output packet is being sent.

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 4 of 6)

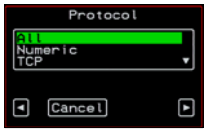
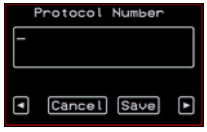
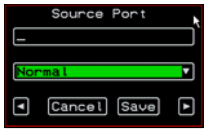
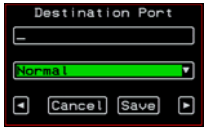
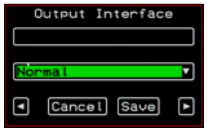
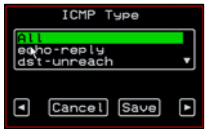
Screen	Description
Protocol 	Choices are “All,” “Numeric,” “TCP,” “UDP,” “ICMP.”
Protocol Number 	Appears only if “Numeric” is selected from the “Protocol” menu.
Source Port 	Appears only if “TCP” or “UDP are selected from the “Protocol” menu. The source port number.
Destination Port 	Appears only if “TCP” or “UDP are selected from the “Protocol” menu. The destination port number.
SYN Flag 	“SYN” (synchronize), appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
RST Flag 	“RST” (reset), appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 5 of 6)

Screen	Description
ACK Flag 	"ACK" (acknowledge), appears only if "TCP" is selected from the "Protocol" menu. Options are "Any," "Set," "Unset."
URG Flag 	"URG" (urgent), appears only if "TCP" is selected from the "Protocol" menu. Options are "Any," "Set," "Unset."
FIN Flag 	"FIN" (finish), appears only if "TCP" is selected from the "Protocol" menu. Options are "Any," "Set," "Unset."
PSH Flag 	"PSH" (push), appears only if "TCP" is selected from the "Protocol" menu. Options are "Any," "Set," "Unset."
Input Interface 	Appears only if "All," "Numeric," "TCP," "UDP," or "ICMP are selected from the "Protocol" menu.

Table 7-10: IP Filtering Configuration Screens [OSD] (Sheet 6 of 6)

Screen	Description
Output Interface 	Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP are selected from the “Protocol” menu.
Fragments 	Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP are selected from the “Protocol” menu.
ICMP Type 	Appears only if ICMP is selected from the “Protocol” menu. Choices are listed in Table 7-11 on page 416.

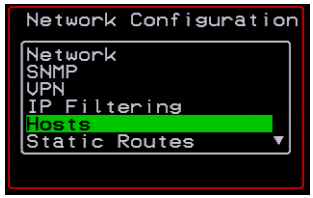
ICMP Type Options are listed in the following table.

Table 7-11: ICMP Type Filtering Options [OSD]

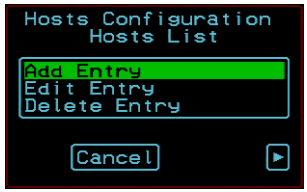
- All
- echo-reply
- dst-unreach (destination-unreachable)
- network-unreach (network-unreachable)
- host-unreach (host-unreachable)
- protocol-unreach (protocol-unreachable)
- port-unreach (port-unreachable)
- fragment needed (fragmentation needed)
- src-rt-failed (source-route-failed)
- network-unknown
- host-unknown
- network-prohibited
- host-prohibited
- TOS-network-unreach (TOS-network-unreachable)
- time-exceeded
- comm-prohibited (communication prohibited)
- host-prec-violation
- precedence-cutoff
- src-quench
- redirect
- network-redirect
- host-redirect
- TOS-network-redir
- TOS-host-redirect
- echo-request
- rt-advertisement
- rt-solicitation
- time exceeded
- ttl-zero-in-transit
- ttl-zero-in-reasm
- parameter-problem
- ip-header-bad
- reqd-opt-missing
- timestamp-req
- timestamp-reply
- addr-mask-req
- addr-mask-reply

Configure>Network>Hosts Screens [OSD]

An administrative user can select the Hosts option from the Network Configuration menu to configure hosts.



Selecting Hosts under Configure>Network brings up the “Hosts List” action menu, as shown in the following figure.



An administrative user can select the options on this menu to add, edit, or delete host entries. Selecting “Edit” or “Delete Entry” brings up the “Select a host” screen shown in the following figure.

The following diagram lists the names of the configuration screens accessed under Configure>Network>Hosts.

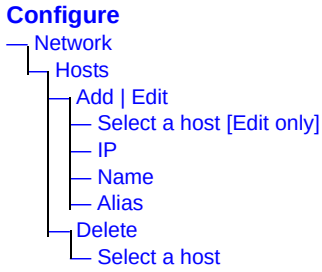
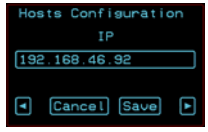
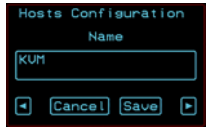


Figure 7-22: OSD Configure>Network>Hosts Screens

See “Configure>Network>Hosts Screens [OSD]” on page 417 for more information.

The following table shows the screens for the Add and Edit options.

Table 7-12: Configure>Network>Hosts Configuration Screens [OSD]

Screen	Description
IP 	IP address of the host
Name 	Hostname of the host
Alias 	Optional alias of the host

Configuring Hosts [OSD]

An administrative user can use the Configure>Network>Hosts screen to configure hosts.

▼ *To Edit a Host [OSD]*

1. Go to: Configure>Network>Hosts.

   The “Hosts List” screen appears.

2. Select “Edit Entry.”

   The Select a Hosts screen appears.

3. Select a hostname from the list.

   The IP screen appears.

4. If desired, change the IP address of the selected host.

   The Name screen appears.

5. If desired, change the hostname.

   The Alias screen appears.

6. If desired, change the alias name for the host.

7. Save the changes.

   The Configuration screen appears.

▼ *To Delete a Host* [OSD]

1. Go to: Configure>Network>Hosts.

   The Hosts List screen appears.

2. Select Delete Entry.

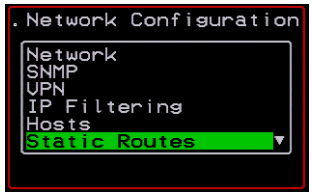
   The Select a Host screen appears.

3. Select a host from the list.

   The Configuration screen appears.

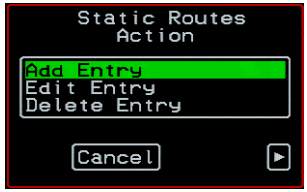
Configure>Network>Static Routes Screens [OSD]

An administrative user can select the Static Routes option from the Network Configuration menu to configure static routes.



If judiciously used, static routes can sometimes reduce routing problems and routing traffic overhead. If injudiciously used, when a network fails, static routes can block packets that would otherwise be able to find alternate routes around the point of failure if dynamic-routing were in effect.

Selecting Static Routes under Configure>Network brings up the Static Routes Action Menu, as shown in the following screen.



The following diagram lists the configuration screens accessed under Configure>Network>Static Routes.

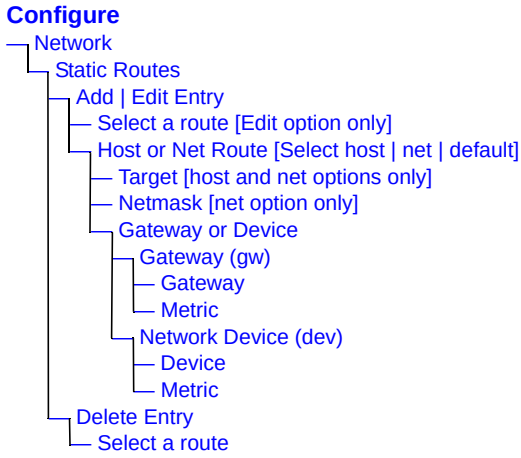


Figure 7-23: OSD Configure>Network>Static Routes Screens

The following table shows the static routes screens that appear when one of the actions (Add, Edit, or Delete) is selected.

Table 7-13: Static Routes Screens [OSD] (Sheet 1 of 2)

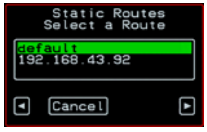
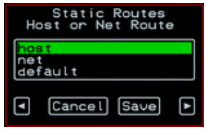
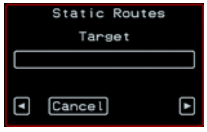
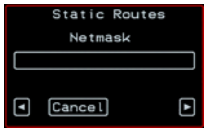
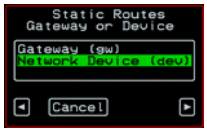
Screen	Description
Select a route 	Appears only when the Edit and Delete options are selected. Choices include the “default” route entry and any previously-configured static routes.
Host or Net Route 	Types of routes: “host,” “net,” or “default.” **Note:** A default route is used to direct packets that are addressed to networks not listed in the routing table.
Target 	IP address for the target host or network.

Table 7-13: Static Routes Screens [OSD] (Sheet 2 of 2)

Screen	Description
Netmask 	Appears only when “net” is selected from the “Host or Net Route” screen. Netmask for the destination.
Gateway or Device 	Two options are: “Gateway (gw)” or “Network Device (dev).”
Gateway 	Appears only when “Gateway (gw)” is selected from the “Gateway or Device” menu. Gateway IP address.
Device 	Appears only when “Network Device” is selected from the “Gateway or Device” menu. Interface name (such as `eth0`).
Metric 	The number of hops to the destination.

Configuring Static Routes [OSD]

An administrative user can use the Static Routes screen to configure static routes.

▼ *To Add a Static Route [OSD]*

1. Go to Configure>Static Routes.

   The Static Routes Action screen appears.

2. Select Add.

   The Host or Net Route screen appears

3. To add a host route, do the following:

   a. Select “host” and press Enter.

      The “Target” screen appears.

   b. On the “Target” screen, enter the IP address for the host.

      The “Gateway or Device” screen appears

   c. If you select “Gateway,” go to Step 6

   d. If you select “Network Device,” go to Step 7

4. To add a network static route, on the Host or Net Route screen do the following:

   a. Select “net” and press Enter.

      The “Target” screen appears.

   b. On the “Target” screen, enter the IP address of the network.

      The “Netmask” screen appears.

   c. Enter the netmask.

      The “Gateway or Device” screen appears

   d. If you select “Gateway,” go to Step 6

   e. If you select “Network Device,” go to Step 7

5. To add a default static route, do the following:

   a. Select “default” and press Enter.

      The “Gateway or Device” screen appears

   b. If you select “Gateway,” go to Step 6

   c. If you select “Network Device,” go to Step 7

6. To add a static route to a gateway, do the following:
   a. Select “Gateway,” and press Enter.

      The “Gateway,” screen appears.

   b. Enter the gateway IP address.

      The “Metric” screen appears.

   c. Skip to Step c.
7. To add a static route to an interface, do the following:
   a. Select “Network Device” and press Enter.

      The “Device” screen appears.

   b. On the “Device” screen, enter the name of the interface and press Enter.

      The Metric screen appears

   c. On the Metric screen, enter a metric.

▼ *To Edit a Static Route [OSD]*

1. Go to: Configure>Static Routes.

   The Static Routes “Action” screen appears.
2. Select Edit.

   The “Select a Route” screen appears.
3. Select a route.

   The “Host or Net Route” screen appears
4. To add a host route, do the following:

   (To add a network route, go to Step 5. To add a default route, go to Step 6.)
   a. Select “host” and press Enter.

      The “Target” screen appears.

   b. On the “Target” screen, enter the host’s IP address.

      The “Gateway or Device” screen appears

c. If you select “Gateway,” go to Step 6

d. If you select “Network Device,” go to Step 7

5. To add a network route, on the “Host or Net Route” screen do the following:

a. Select “net” and press Enter.

The “Target” screen appears.

b. On the “Target” screen, enter the IP address.

The “Netmask” screen appears.

c. Enter the netmask.

The “Gateway or Device” screen appears

d. If you select “Gateway,” go to Step 6

e. If you select “Network Device,” go to Step 7

6. To add a default static route, do the following:

a. Select “default” and press Enter.

The “Gateway or Device” screen appears

b. If you select “Gateway,” go to Step 6

c. If you select “Network Device,” go to Step 7

7. To add a static route to a gateway, do the following:

a. Select “Gateway” and press Enter.

The “Gateway” screen appears.

b. Enter the gateway’s IP address.

The “Metric” screen appears.

c. Skip to Step c

8. To add a static route to a device, do the following:

a. Select “Network Device” and press Enter.

The “Device” screen appears.

b. On the “Device” screen, enter the device identifier.

The “Metric” screen appears.

9. On the “Metric” screen, enter a metric.

▼ *To Delete a Static Route [OSD]*

1. Go to: Configure>Static Routes.

   The “Static Routes Action” screen appears.

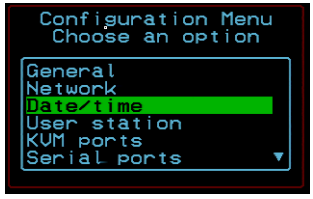
2. Select “Delete Entry.”

   The “Select a Route” screen appears.

3. Select a route to delete and press Enter to save changes.

Configure>Network>Date/time Screens [OSD]

An administrative user can select the Date/time option from the OSD Configuration menu to either configure an NTP server or manually set the date and time.



Selecting Date/time under Configuration>Network brings up the NTP menu, as shown in the following screen.

The following diagram lists the names of the configuration options accessed from the Configure>Date/time menu.

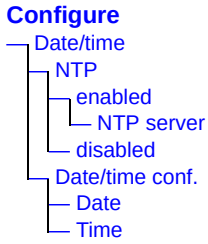
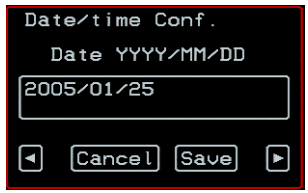
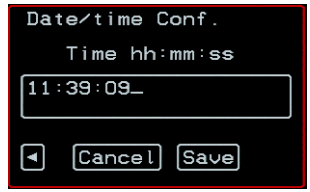


Figure 7-24: OSD Configure>Date/time Screens

If NTP is enabled, the following screen appears for entering the IP address of the NTP server.

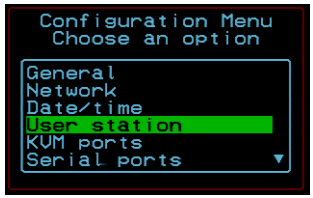
If NTP is disabled, the following series of two screens appears to allow you to enter the date and time manually.





Configure>User Station Screens [OSD]

An administrative user can select the User Station option from the OSD Configuration menu to redefine the parameters that apply to a Local User session (when a user is accessing the OSD through a Local User station that is directly connected to the OnSite).



The following diagram lists the configuration screens accessed through the Configure>User station option. All the screens that appear after the "Keyboard type" screen are for optionally redefining the command key portion of AlterPath Viewer hot keys: "Quit," "Power Management," "Mouse/Keyboard Reset," "Video Configuration," "Switch Next," "Switch Previous," and "Port Info." See "Configuring Keyboard Shortcuts (Hot Keys)" on page 63 for details, if needed.

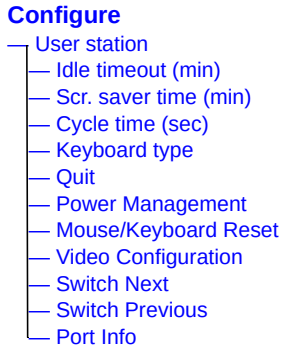


Figure 7-25: OSD Configure>User Station Screens

See "Configuring User Station Screens [OSD]" on page 431 for more information.

The following table shows the user station configuration screens.

Table 7-14: User Station Configuration Screens [OSD] (Sheet 1 of 3)

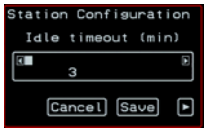
Screen	Description
Idle timeout 	The period of inactivity before the user is logged out from the OSD. Default = 3 minutes.

Table 7-14: User Station Configuration Screens [OSD] (Sheet 2 of 3)

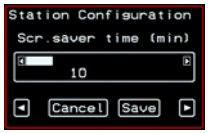
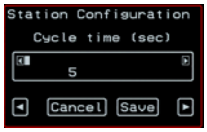
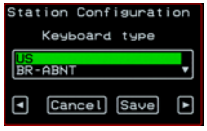
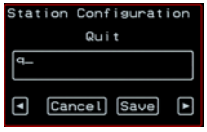
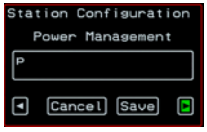
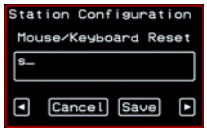
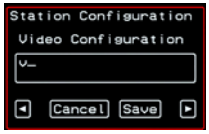
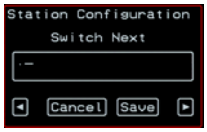
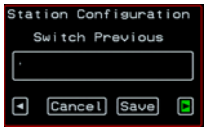
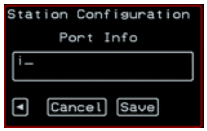
Screen	Description
Scr. saver timeout 	The period of inactivity before the screen saver starts. Default = 10 minutes.
Cycle time (sec) 	The number of seconds each server is viewed while the user is cycling from one port to another. Default = 5 seconds. See “To Cycle Through All Authorized KVM Ports” on page 96 for instructions on how to cycle through the servers.
Keyboard Type 	The type of keyboard connected to the Local User management port of the OnSite. • US [Default] • BR-ABNT • BR-ABNT2 • Japanese • German • Italian • French • Spanish
Quit 	Redefine the command key for the KVM connection quit hot key.
Power Management 	Redefine the command key portion of the KVM connection power management hot key.

Table 7-14: User Station Configuration Screens [OSD] (Sheet 3 of 3)

Screen	Description
Mouse/Keyboard 	Redefine the command key portion of the KVM connection mouse/keyboard reset hot key.
Video 	Redefine the command key portion of the KVM connection video brightness and contrast hot key.
Switch Next 	Redefine the command key portion of the AlterPath Viewer switch next hot key.
Switch Previous 	Redefine the command key portion of the AlterPath Viewer switch previous hot key.
Port Info 	Redefine the command key portion of the AlterPath Viewer port info hot key.

Configuring User Station Screens [OSD]

An administrative user can use the screens under Configure>User station to configure session parameters for the local user connection.

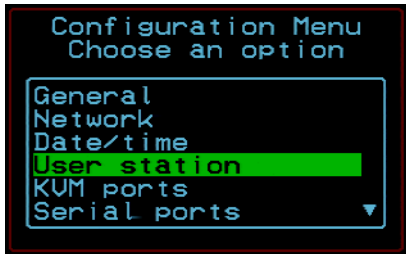


Figure 7-26: Selecting OSD Configure>Date/time

The following table lists the task available in the User Station screens and where to find more information.

Task	Where Documented
Specify the period of inactivity before the session is ended. The default is three minutes.	“To Specify the User Station Idle Timeout” on page 433.
Specify the period of inactivity before the screen saver starts. The default is 10 minutes.	“To Specify the User Station Screen Saver Idle Timeout Period” on page 434
Specify the time each server is viewed while the user is cycling from one port to another. The default cycle time is 3 seconds. See “To Cycle Through All Authorized KVM Ports” on page 96 for instructions on how to cycle through the servers.	“To Configure the User Station: Cycle Time [OSD]” on page 434

Task	Where Documented
Specify the type of keyboard connected to the Local User management port of the OnSite. • US • BR-ABNT • BR-ABNT2 • Japanese • German • Italian • French • Spanish	"To Specify the Users Station Keyboard Type [OSD]" on page 435
Redefine the command key for the quit keyboard shortcut.	"To Specify the User Station Quit Command Key [OSD]" on page 436
Redefine the command key for the power management keyboard shortcut.	"To Configure the User Station Power Management Command Key [OSD]" on page 483
Redefine the command key for the mouse/ keyboard sync keyboard shortcut.	"To Specify the User Station Mouse/ Keyboard Reset Command Key [OSD]" on page 484
Redefine the command key for the video configuration keyboard shortcut.	"To Specify the User Station Video Configuration Command Key [OSD]" on page 485
Redefine the command key for the switch next keyboard shortcut.	"To Specify the User Station Switch Next Command Key [OSD]" on page 485
Redefine the command key for the switch previous keyboard shortcut.	"To Specify the User Station Switch Previous Command Key [OSD]" on page 486
Redefine the command key for the port info keyboard shortcut.	"To Specify the Keys Used in the Command Key Portion of the Port Info Keyboard Shortcut [OSD]" on page 487

Configure>User Station: Idle Timeout [OSD]

The system logs out users after a defined period of inactivity. The default is three minutes. An administrative user can use the User Station>Idle Timeout screen to redefine the idle timeout minutes.

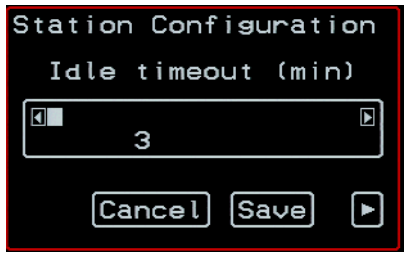


Figure 7-27: Configure>User Station>Idle Timeout

▼ *To Specify the User Station Idle Timeout*

1. Go to: Configure>User station

   The Idle Timeout screen appears.

2. Use the right and left arrows to increase or decrease the time in minutes.
3. Select the next arrow button to go to the Screen Saver Time screen or Esc.

Configure>Users Station: Scr. Saver Idle Timeout [OSD]

The system activates a screen saver after a defined period of inactivity. The default is 10 minutes. An administrative user can use the User Station>Scr. saver screen to redefine the number of idle minutes before the screen saver starts.

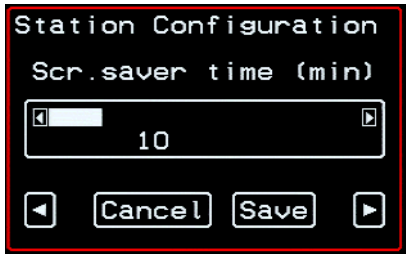


Figure 7-28: Configure>User Station: Scr. Saver Timeout

▼ *To Specify the User Station Screen Saver Idle Timeout Period*

1. Go to: Configure>Users station>Idle Timeout>Scr. Saver Time.
2. Use the forward or back arrows at the end of the scale to adjust the time in minutes.
3. Select the next arrow button to go to the Cycle Time screen.

Configure>Users Station>Cycle Time [OSD]

An administrative user can use the Cycle Time screen to set the time that each server is viewed while the user is cycling from one port to another. The default cycle time is 3 seconds.

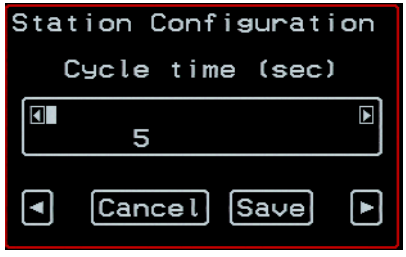


Figure 7-29: Configure>User Station: Cycle Time Screen

▼ *To Configure the User Station: Cycle Time [OSD]*

1. Go to: Configure>Users station>Idle Timeout>Screen Saver Time>Cycle Time.

2. Use the forward or back button to adjust the time in minutes.
3. Select the next arrow button to go to the Keyboard Type screen.

Configure>Users Station: Keyboard Type [OSD]

An administrative user can use the keyboard type screen to configure the type of keyboard connected to the Local User management port of the OnSite.

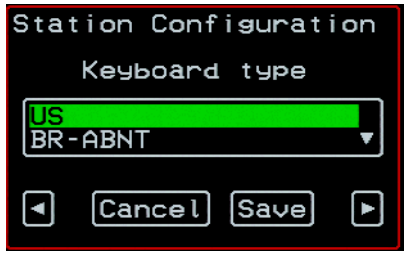


Figure 7-30: Configure>User Station: Keyboard Type Screen

▼ *To Specify the Users Station Keyboard Type [OSD]*

1. Go to: Configure>User Station>Idle Timeout>Scr.Saver Time>Cycle Time>Keyboard Type.
2. Select the keyboard type that matches the one connected to the Local User ports.
3. Select the next arrow button to go to the Quit screen.

Configure>Users Station: Quit Command Key [OSD]

An administrative user can use the Quit screen to redefine the Command Key portion of the quit hot.

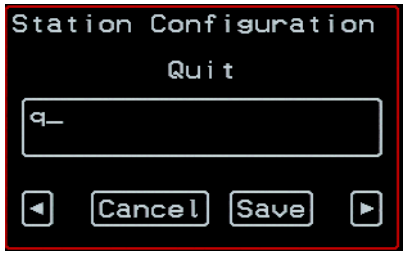


Figure 7-31: Configure>User Station: Quit Screen

▼ *To Specify the User Station Quit Command Key [OSD]*

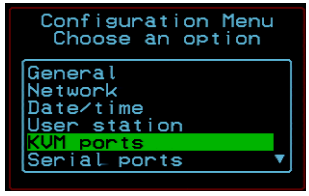
1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit.

   The Quit screen appears.

2. Type the letter to be used for the command key in the quit hot key.
3. Select the next arrow button to go to the Power Management screen.

Configure>KVM Ports Screens [OSD]

An administrative user can select the KVM Ports option on the OSD Configuration Menu to configure KVM ports.



The following diagram lists the configuration screens accessed through the Configure>KVM ports option.

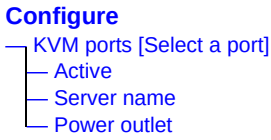


Figure 7-32: OSD Configure>KVM Ports Screens

The following table shows the KVM port configuration screens.

Table 7-15: KVM Port Configuration Screens [OSD] (Sheet 1 of 2)

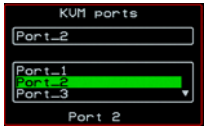
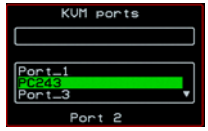
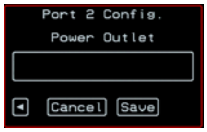
Screen	Description
KVM ports 	Lists all KVM ports by their default names or administratively-defined aliases.
Active 	Choices are “Yes” and “No” to activate or deactivate the selected KVM port.
Server name 	Allows you to assign a descriptive alias, such as the name of the server to which the selected KVM port is connected. Only alpha-numeric characters, hyphens (-), and underscores (_) are accepted. The new alias replaces the default port name in the list of ports as shown here: 

Table 7-15: KVM Port Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
Power Outlet 	Allows you to enter one or more numbers that identify power outlet or outlets into which the server that is connected to this KVM port is plugged. When IPDUs are daisy-chained, the outlets on the second and subsequent IPDUs are numbered sequentially. AUX port 1 is assumed because power management while connected to servers that are connected to KVM ports can only be done when the servers are plugged into outlets on an IPDU on AUX port 1. When multiple IPDUs are daisy-chained, outlets are numbered sequentially. For example, the fourth outlet on a second daisy-chained IPDU when the first IPDU has eight outlets is specified as “12,” and the next outlet is specified as “13,” in the format: “12, 13.” See “Power Management While Connected to Devices” on page 51 for details. Also see “To Power On, Off, or Cycle a Server While Connected to a KVM Port” on page 99, if needed.

Configuring KVM Ports [OSD]

An administrative user can use the screens under Configure>KVM ports to do the following configuration:

- Enable or disable a KVM port
- Assign an alias to a KVM port
- Enable an authorized user connected to a server through a KVM port to perform power management, when the server is plugged into an IPDU connected to an AUX port

▼ *To Select a KVM Port to Be Configured* [OSD]

1. Go to: Configure>KVM Ports.

   The KVM ports screen appears.

2. To select the port you wish to configure, do one of the following:

- Type the first letters of the port name until the desired port is highlighted in the port list box.

  This field is case-sensitive.

- OR -

- Select the desired port using the port list box.

3. Press Enter to go to the KVM Ports Active screen.

▼ *To Activate a KVM Port* [OSD]

1. Go to: Configure>KVM Ports>Active.

   The KVM Ports Active screen appears.

2. Select Yes or No to activate or disable the currently selected port.
3. Select the next arrow button to go to the Server Name screen.

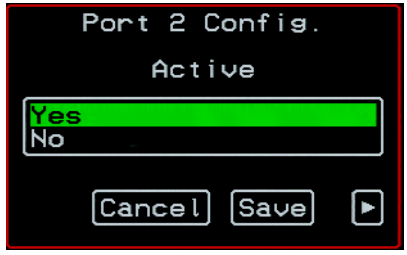


Figure 7-33: Configure>KMP Ports: Server Name

The alias can be the name of the server to which the port is connected, or it can be any other name to identify the server connected to the port.

▼ *To Assign a Server Name to the Port* [OSD]

1. Go to Configure>KVM Ports>Active>Server Name.

   The Server Name screen appears.

2. Type the name of the server to which the currently selected port is connected, or use another name to identify the server.

   Use only alpha-numeric characters, hyphens (-), and underscores (_).

3. Do one of the following:

a. To verify the new server name, select Save.

The KVM Ports selection screen appears with new port alias listed.

- OR -

b. Select the right arrow button to go to the Power Outlet screen.

▼ *To Enable Power Management Through a KVM Port [OSD]*

See “IPDU Power Management (OSD)” on page 382 for background information, if needed. The prerequisites for this procedure are that you know the following:

- The number of the AUX port where the IPDU is connected
- The number of the outlet(s) into which the server is plugged that is connected to the selected port.

You can specify up to two outlets.

1. Go to: Configure>KVM ports, select a Server Name/Port Number, and then go to Server Name>Active>Power Outlet.

   The Power Outlet screen appears with the port alias or number at the top.

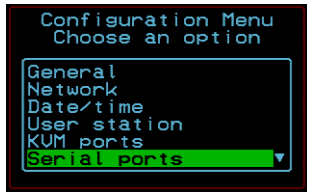
2. Type the outlet number(s).

   If the server connected to the KVM port is plugged into two different outlets, you can enter two outlets per port; use a space to separate them. Enter the outlet number(s) using the format: *A*:*N*, where *A* is the number of the AUX port to which the PM is connected (either 1 or 2) and *N* is the number of the outlet. If more than one IPDU is daisy chained to an AUX port, specify the outlet numbers incrementally.

3. Select Save.

Configure>Serial Ports Screens [OSD]

An administrative user can select the Serial Ports option on the OSD Configuration Menu to configure serial ports.



Note: The OSD does not support connecting to serial ports. However, authorized users can use the Web Manager to connect to a serial port once the serial port access permissions have been configured either using this screen or through the Web Manager.

The following diagram lists the configuration screens accessed through the Configure>Serial ports option.

Configure
- Serial ports
  - [Select a port]
  - Choose an option
    - Connection protocol
    - Activate [only when a single port is selected]
    - Server alias [only when a single port is selected]
    - Config power outlet [only when a single port is selected]
    - Baud rate
    - Port permissions
      - Port access list
      - Grant/Deny access
      - Exit
    - Authentication
    - Exit
  - Exit

Figure 7-34: OSD Configure>Serial Ports Screens

The following table shows the serial port configuration screens.

Table 7-16: Serial Port Configuration Screens [OSD] (Sheet 1 of 4)

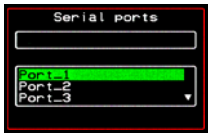
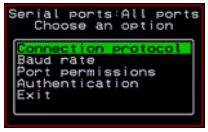
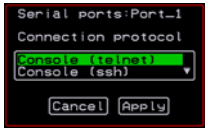
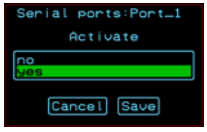
Screen	Description
Serial ports 	Select a serial port. Type the first letters of the port name until the desired port is highlighted in the list, type capital A to highlight “All ports” (the port name field is case-sensitive), or select the desired port name or “All ports” from the list.
Choose an option 	A list of serial port configuration parameters that you can redefine to match the device that is connected to the serial port, which are defined in the following rows.
Connection protocol 	A list of connection protocols. Default = Console (telnet). Choose the appropriate connection protocol for the type of device connected to the serial port. See Table 6-12, “Protocols for Devices With Console Ports Connected to Serial Ports,” on page 232, Table 6-13, “Protocols for Dumb Terminals Connected to Serial Ports,” on page 233, Table 6-15, “Protocols for Serial Ports Connected to Modems or IPDUs,” on page 235 for details.
Activate 	Appears only when a single port is selected. Default = yes.

Table 7-16: Serial Port Configuration Screens [OSD] (Sheet 2 of 4)

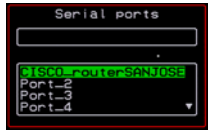
Screen	Description
Server alias 	Appears only when a single port is selected. Lets you assign a descriptive alias to the selected serial port, such as the name of the device to which the selected port is connected. The name must consist only of alpha-numeric characters, hyphens (-), and underscores (_).The new alias replaces the default port name in the list of serial ports as shown here: 

Table 7-16: Serial Port Configuration Screens [OSD] (Sheet 3 of 4)

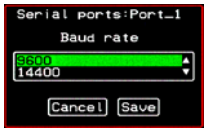
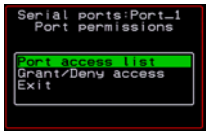
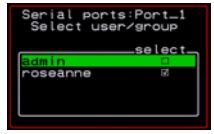
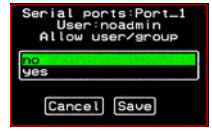
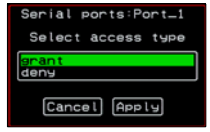
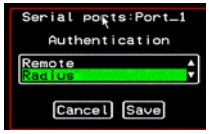
Screen	Description
Config power outlet 	Appears only when a single port is selected. Allows you to enter one or more numbers that identify a power outlet or outlets where the device that is connected to this serial port is plugged. The power outlets must be on an IPDU that is physically connected to AUX ports 1 or 2 or to any serial port, and the ports must be configured for power management. Use the format *AN.N* to specify the outlet in the "Config power outlet" field, where: *A* is either the letter "a" (for AUX port) or the letter "s" (for serial port), the first *N* before the dot (.) is the number of the port, and the second *N* is the number of the outlet. For AUX ports, you can enter either numbers 1 or 2. For serial ports, you can enter any valid serial port number. When IPDUs are daisy-chained, the outlets on the second and subsequent IPDUs are numbered sequentially. You can enter up to twenty characters, so you can specify up to four outlets. For example, if a single IPDU is connected to AUX port 2 and a server connected to the selected port is plugged into the third, fourth, fifth, and sixth outlets on the IPDU, you would enter: **`a2.3,a2.4,a2.4,a2.5`**. For another example, if four IPDUs are daisy-chained on serial port 3 and the first three IPDUs have eight ports, and if a device connected to the selected serial port is plugged into the second and third outlets on the fourth IPDU, you would enter: **`s3.26,s3.27`**. See "Power Management While Connected to Devices" on page 51 for details. Also see "To Power On, Off, or Cycle a Server While Connected to a KVM Port" on page 99, if needed.
Baud rate 	The baud rate that matches the baud rate of the device connected to the selected serial port or all serial ports. Default = 9600. Baud rate options range from 2400–921600 Kbps.

Table 7-16: Serial Port Configuration Screens [OSD] (Sheet 4 of 4)

Screen	Description
Port permissions 	Choices are: “Port access list” or “Grant/Deny access.” By default, no regular users are authorized to access serial ports. To authorize regular users to access serial ports, the OnSite administrator must use this screen or the Web Manager. Selecting “Port access list” brings up the following **Select user/group** and **Allow user/group** screens. You can either grant access or deny access to a user or group. Granting access to any user or group to the port has the effect of denying access to all other users, including “root” and “admin.”   Selecting “Grant/Deny” access brings up the **Select access type** screen. Use this screen to give all users the same level of access. 
Authentication 	Authentication method to apply to the selected serial port or ports. Default = Local. See “OnSite Authentication Options” on page 7 for an overview of authentication on the OnSite. Authentication options for serial ports are described in Table 1-3, “Supported Authentication Types,” on page 9. A server must be configured for any authentication method assigned in this screen except Local. See Table on page 470 for links to procedures for setting up authentication servers for each type of method.

Configuring Serial Ports [OSD]

An administrative user can use the “Serial Ports” screen to configure serial ports as follows:

- Choose a connection protocol: telnet, ssh, raw, or power management
- Enable or disable one or all serial ports
- Assign an alias to one serial port at a time
- Enable power management on a serial port by an administrator who is connected to the serial port
- Set the baud rate for one or all serial ports
- Set user and group access permissions for one or all serial ports
- Set authentication for one or all serial ports

See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446 for how to start and for links to the procedures for performing the previously-listed tasks.

▼ *To Select a Serial Port or Ports to be Configured* [OSD]

1. Go to: Configure>Serial ports.

   The Serial ports screen appears with a list of all the serial ports and an option called “All ports.”

2. To select a port or all ports, do one of the following:

   - Type the first letters of the port name until the desired port is highlighted in the list or type capital A to highlight “All ports”

     The port name field is case-sensitive.

   or

   - Select the desired port name or “All ports” from the list.

Note: Selecting “All ports” allows you to configure all ports the same.

---

3. Press Enter.

The “Serial ports” menu appears with the name of the selected port displayed on the first line of the screen.

4. Go to “To Configure a Connection Protocol for a Serial Port [OSD]” on page 447

▼ *To Configure a Connection Protocol for a Serial Port* [OSD]

1. Select a serial port or all ports.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.

2. Select “Connection Protocol” from the list of options.

   The Connection protocol screen appears with a list of protocols.

3. Select the connection protocol that matches the type of device that is connected to the serial port.

▼ *To Assign an Alias to a Serial Port* [OSD]

1. Select a single serial port.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.

2. Select “Server alias.”

   The “Server alias” screen appears.

3. Enter the desired alias.

   Use only alpha-numeric characters, hyphens (-), and underscores (_).

4. Save the changes.

   The “Serial ports” screen appears with the new alias replacing the old port name.

▼ *To Enable Power Management Through a Serial Port* [OSD]

This procedure assumes the following:

- The device that is connected to the serial port currently being configured is plugged into one or more outlets on an IPDU
- The IPDU is physically connected to an AUX port or serial port on the OnSite
- The AUX port or serial port where the IPDU is connected has been configured for power management
- You know the number of the port where the IPDU is connected and the number(s) of the outlet(s) into which the device is plugged.

1. Select a single serial port.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.

2. Select “Config power outlet.”

   The “Config power outlet” screen appears.

3. Enter the outlet number(s), using the format *a|sN.N* and using commas to separate multiple outlet identifiers up to a total of 20 characters.

   For example: **a2.3,a2.4,a2.4,a2.6** or **s3.34,s3.37**.

4. Save the changes.

▼ *To Specify the Baud Rate for Serial Port(s)* [OSD]

1. Select a serial port or all serial ports.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.

2. Select Baud rate from the “Serial ports” menu.

   The Baud rate screen appears.

3. Select a baud rate from the menu.

4. Save the changes.

▼ *To Configure Who Can Access Serial Ports* [OSD]

After selecting a serial port, an administrative user can use the options on the “Port permissions” screen to grant or deny access by users or groups to a selected serial port or to all serial ports. By default, all users can access all serial ports. Adding a user or group to the port access list has the following effects:

- The user or group is granted access to the port unless the additional step is taken to deny access.
- All other users are denied access to the port, even “root” and “admin.”

1. Select a serial port or all serial ports.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.

2. Select “Port permissions” from the “Serial ports” menu.

   The “Port permissions” screen appears.

3. Select “Port access list.”

   The “Select user/group” screen appears displaying the names of configured users. By default, the checkboxes next to each name in the “access” column are not checked, and no regular users have access to the selected port or ports.

4. Select a user or group name from the menu.

   The “Allow user/group” screen appears.

5. Select “yes” from the menu.

6. Select “Apply” to save the changes.

   The “Select user/group” screen appears.

7. Press the Esc key.

   The “Port permissions” screen appears.

8. To deny access to a user or grant access to a user who has previously been denied access, select “Grant/deny access.”

   The “Select access type” screen appears.

9. Select “grant” or “deny” as desired.
10. Select “Apply” to save the changes.

    The “Port permissions” screen appears.
11. Select “Exit.”

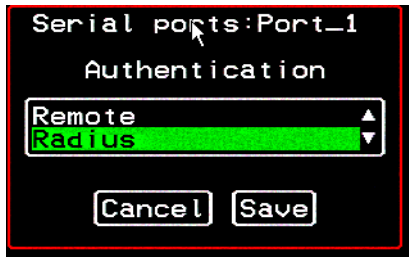
▼ *To Specify an Authentication Method for Serial Ports* [OSD]

This procedure assumes you have already configured a server for the authentication method you assign in this screen. See “To Configure an Authentication Type for Direct KVM Port Access” on page 392

1. Select a serial port or all serial ports.

   See “To Select a Serial Port or Ports to be Configured [OSD]” on page 446, if needed.
2. Choose “Authentication” from the “Serial ports” menu.

   The “Authentication” menu appears.

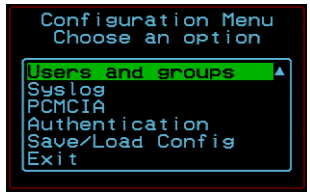


3. Select the desired authentication method for a selected serial port or all ports.

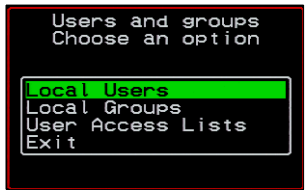
   See “OnSite Authentication Options” on page 7 for an overview of authentication on the OnSite. See Table 7-29 on page 492 for links to procedures for setting up authentication servers for each type of method.

Configure>Users and Groups Screens [OSD]

An administrative user can choose the “Users and groups” option from the OSD Configuration menu to configure users, groups, and KVM port permissions.The following figure displays the Users and Groups screen.



When “Users and Groups” is selected, the “Choose an option” screen appears, as shown in the following screen example. The “Local Users” option is for configuring users; the “Local Groups’ option is for configuring groups, and the “User Access Lists” option is for configuring users’ and groups’ access to KVM ports.



The following diagram lists the configuration screens accessed through the Configure>Users and Groups options:

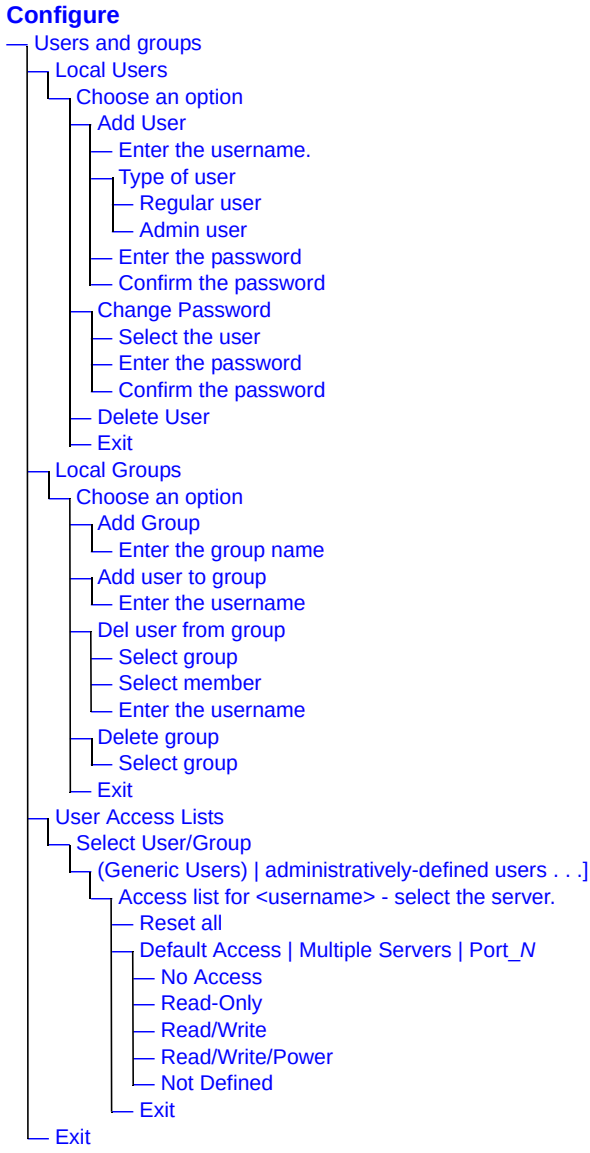


Figure 7-35: OSD Configure>Users and Groups Screens

The following table shows the configuration screens that appear when the “Local Users” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-17: Local Users Configuration Screens [OSD] (Sheet 1 of 2)

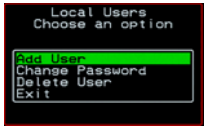
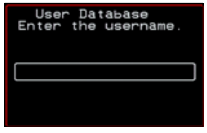
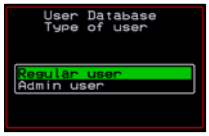
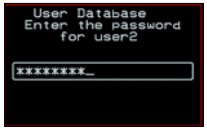
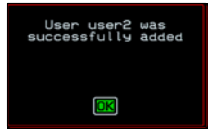
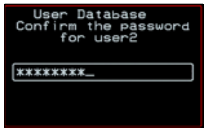
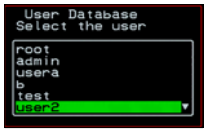
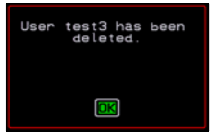
Screen	Description
Choose an option 	Options are: “Add User,” “Change Password,” “Delete User,” or “Exit.”
User Database Enter the username 	Appears only when “Add User” is selected.
Type of user 	Appears only when “Add User” is selected. Options are: “Regular User” and “Admin user.”
Enter the password 	Appears only when “Add User” or “Change Password” are selected. **Note:** Passwords are case sensitive. When the password is successfully confirmed, the following dialog box appears. 
Confirm the password 	

Table 7-17: Local Users Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
Select the user 	Appears only when “Change Password” or “Delete User” are selected. When “Delete User” and then a username are selected, a confirmation screen like the following appears: 

The following table shows the configuration screens that appear when the “Local Groups” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-18: Local Groups Configuration Screens [OSD] (Sheet 1 of 2)

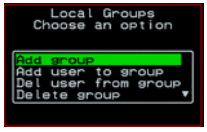
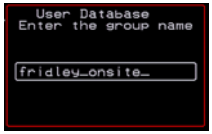
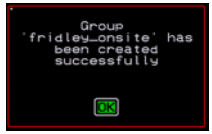
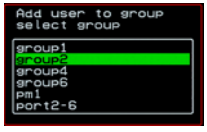
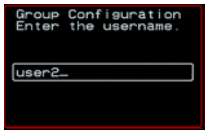
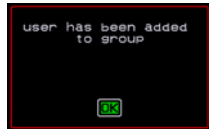
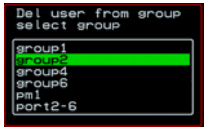
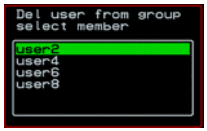
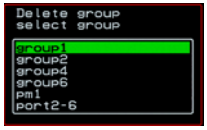
Screen	Description
Choose an option 	Options are “Add group,” “Add user to group,” “Del. user from group,” “Delete group,” and Exit
Enter the group name 	When “Add group” is selected. After the group name is entered, a confirmation screen like the following appears. 
select group 	When “Add user to group” is selected

Table 7-18: Local Groups Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
Enter the username 	When “Add user” or “Add user to group” are selected. To add multiple users, use a comma to separate each username. When the user is successfully added, the following confirmation screen appears. 
Delete user from group **select group** 	When “Del user from group” is selected.
select member 	When “Del user from group” and a username are selected, the user is removed from the group, and the following confirmation screen appears: 
Delete group **select group** 	When “Delete group” and a group name are selected, the following confirmation screen appears. 

An administrative user can use the User Access Lists menu to view and change KVM port access permissions for the Default User and all

administratively-configured users and groups. See “Understanding KVM Port Permissions” on page 32 for details.

The following table shows the configuration screens related to setting KVM port access permissions when the “User Access List” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-19: User Access List KVM Port Permissions Configuration Screens [OSD] (Sheet 1 of 3)

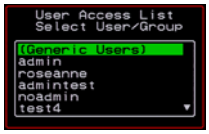
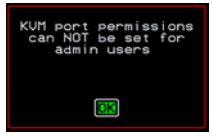
Screen	Description
Select User/Group 	“[Generic Users]” and any administratively-defined users and groups are listed, along with the “Exit” option. The Generic Users’ permissions apply to all users except for “admin” and any users in the “admin” group. By default, the Generic Users’ default permission is “No Access,” and no KVM port permissions are defined. Therefore, by default, any regular users that may be added cannot access any KVM ports. The OnSite administrator can configure access to KVM ports for added regular users by: • By selecting “[Generic Users]” and modifying the permissions that apply to all users who have not been configured with specific permissions - OR - • By configuring specific permissions for one or more individual users or groups (by selecting a single port or the “Multiple servers” option) **Note:** The KVM port access permissions for “admin” or for anyone in the admin group cannot be changed. The “admin” is not listed, but if any other administrative user’s username is selected, the following screen displays: 

Table 7-19: User Access List KVM Port Permissions Configuration Screens [OSD] (Sheet 2 of 3)

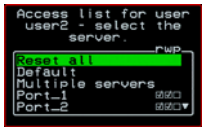
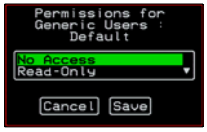
Screen	Description
Access list for *username* - select the server 	The access list includes the “Reset all,” “Default,” “Multiple servers,” and “Exit” options along with individual KVM ports. The “Default” option defines access permissions for all KVM ports, which apply unless the user has specific access permissions for any KVM ports. For a new user, because “Default Access,” is not defined, and also because no permissions are specified for that user’s access to any specific port, the Generic Users’ permissions apply. A series of three checkboxes appear to the right of each entry that has specific permissions (as defined in the following row). If a port has “No Access” defined, the checkboxes are empty. The headings for the checkboxes are: `rwp` for read, write, and power, and the boxes are checked appropriately when any of these permissions are defined. For example, in the screen to the left, the `r` and `w` boxes are checked next to “Port_1” and “Port_2,” which indicates that the user has read-write access to these ports. If “Reset all” is selected, the following confirmation screen appears. 

Table 7-19: User Access List KVM Port Permissions Configuration Screens [OSD] (Sheet 3 of 3)

Screen	Description
Permissions for *username*: *port_number* or for *username*: followed by another Access list option, such as "Default" or "Multiple Servers" 	The permissions from this menu can be configured to be "Default" permissions for all ports, applied to Multiple Servers, or applied to a selected port. Permissions options are "No Access," Read-Only," "Read Write," "Read/Write/Power," and "Default." When "Default" was selected on the previous menu, the "Not Defined" option also appears on the menu.

Configuring Users and Groups [OSD]

An administrative user can use can use the "Users and Groups" screen from the Configuration Menu to specify users and permissions.

The following table lists the configuration tasks you can perform:

Task	Where Documented
Add a user.	"To Configure Users [OSD]" on page 459 "To Add a User [OSD]" on page 460
Change a user's password.	"To Change a Password [OSD]" on page 460
Delete a user.	"To Delete a User [OSD]" on page 460
Add a group.	"To Add a Group [OSD]" on page 461
Add a user to a group.	"To Add a User to a Group [OSD]" on page 461
Delete a user from a group.	"To Delete a User from a Group [OSD]" on page 462

Task	Where Documented
Delete a group.	“To Delete a Group [OSD]” on page 462
Add a user to the User Access List.	“To Give a User Access to KVM Ports [OSD]” on page 463
Edit user or group permissions.	“To Edit a User or Group’s Access to KVM Ports [OSD]” on page 464
Apply permissions to the Generic user group.	“To Edit Permissions for the Generic User [OSD]” on page 465
Delete a user from the User Access List.	“To Delete a User From the User Access List [OSD]” on page 465

To understand how the hierarchy of permissions work when creating user permissions between groups and the generic user, refer to “OnSite Port Permissions” on page 32.

Note: The term “local” is used to refer to the fact that account information for users created in the OSD are stored locally in configuration files on the OnSite.

▼ *To Configure Users [OSD]*

1. Go to: Configure>Users and Groups>Local Users.

   The “Local User – Choose an Option” screen appears.

2. Choose one of the following options:

Task	Where Documented/Notes
Add User	“To Add a User [OSD]” on page 460
Change Password	“To Change a Password [OSD]” on page 460
Delete User	“To Change a Password [OSD]” on page 460
Exit	Return to the previous menu

▼ To Add a User [OSD]

1. Go to Configure>Users and Groups>Local Users>Add User.

   The Enter the Username screen appears.

2. Type in the username in the input box and press <Enter>.

Note: Usernames are case sensitive.

   The Enter the Password screen appears.

3. Enter the user's password.

Note: Passwords are case sensitive.

   The Confirm the Password screen appears.

4. Re-enter the password.
5. Click OK to return to the previous menu.

▼ To Change a Password [OSD]

1. From the OSD Main Menu, go to Configure>Users and Groups>Local Users>Change Password..

   The "Select the user" screen appears.

2. Select the user name.
3. Enter a new password.
4. Re-enter the new password.

   A confirmation message appears.

5. Select OK to return to the previous menu.

▼ To Delete a User [OSD]

1. Go to Configure>Users and Groups>Local Users>Delete User.

   The Select the User screen appears.

2. Select the user that you wish to delete and press <Enter>.

The system displays a message to confirm your deletion.

3. Click **OK** to return to the main menu.

▼ To Configure Groups [OSD]

1. Go to: Configure>Users and Groups>Local Groups

   The Local Groups – Choose Option screen appears

2. Go to one of the group configuration tasks listed in the following table.

Table 7-20: Tasks for Configuring Groups [OSD]

Task	Where Documented/Notes
Add a local group	“To Add a Group [OSD]” on page 461
Add a user to a group	“To Add a User to a Group [OSD]” on page 461
Delete a user from a group	“To Delete a User from a Group [OSD]” on page 462
Delete a group	“To Delete a Group [OSD]” on page 462
Exit	Return to the previous menu

▼ To Add a Group [OSD]

1. Go to Configure>Users and Groups>Local Groups>Add Group.

   The “Enter the Group Name” screen appears.

2. Type in the group name you wish to add and press <Enter>.

   A confirmation message screen appears

3. Click OK to return to the main menu.

▼ To Add a User to a Group [OSD]

1. Go to Configure>Users and Groups>Local Groups>Add user to group.

   The Add User to Group - Select Group screen appears.

2. Select the group to which you wish to add the user and press <Enter>.

   The “Group Configuration - Enter the Username” screen appears.

3. Enter the username of the user to add to the group and press “Enter.”

   To add multiple users, use a comma to separate each username.

   A confirmation message appears.

4. Click OK to return to the main menu.

▼ To Delete a User from a Group [OSD]

1. Go to Configure>Users and Groups>Local Groups>Delete User from Group.

   The “Delete User from Group - Select Group” screen appears.

2. Select from the list the group that you wish to delete and press <Enter>.

   The Delete User from Group - Select Member screen appears.

3. Select the user that you wish to delete from the group and press <Enter>.

4. Click OK to return to the main menu.

▼ To Delete a Group [OSD]

1. Go to Configure>Users and Groups>Local Groups>Delete Group.

   The Delete Group - Select Group screen appears.

2. Select the group to delete and press Enter.

   A confirmation message appears.

3. Click OK to return to the main menu.

▼ To Choose an Option for Adding, Editing, or Deleting User and Group KVM Port Access Permissions [OSD]

1. Go to Configure>Users and Groups>User Access Lists.

2. Choose from the following tasks:

Task	Where Documented/Notes
Specify KVM port access permissions for a user	"To Give a User Access to KVM Ports [OSD]" on page 463
Edit user or group permissions	"To Edit a User or Group's Access to KVM Ports [OSD]" on page 464
Apply permissions to the Generic user group.	"To Edit Permissions for the Generic User [OSD]" on page 465
Delete a user from the User Access List.	"To Delete a User From the User Access List [OSD]" on page 465
Exit	Return to the previous menu.

▼ *To Give a User Access to KVM Ports [OSD]*

1. Go to Configure>Users and Groups>User Access List>Add User.

   The User Access List - Enter the Username screen appears.

2. Enter the username of the user to add.

   The Access List for User - Select the Server screen appears. The user's current KVM port access permissions are shown as checkboxes under three columns "rwp." "rwp" indicates the type of access: read, write, or power management.

3. To choose default permissions for the user, choose "Default" from the list.

4. To specify specific access permissions for a KVM port, select the KVM port number or port alias and press "Enter."

   The Permission for User screen appears.

5. Select the type of permission you wish to assign: "read only," "read/write," "read/write/power."

6. Save the changes.

▼ To Edit a User or Group's Access to KVM Ports [OSD]

1. Go to Configure>Users and Groups>User Access List.
2. On the "User Access List - Select the User" screen, select the user or group and press "Enter."

   The "Access List for User - Select the Server" screen appears.
3. To choose default permissions for the selected user or group, choose "Default" from the list.
4. To specify access permissions to individual KVM ports for the selected user or group, do the following:

   a. Select a port number or alias.

      The Permissions screen appears displaying the selected user name and the selected port number or port alias in the heading.

   b. Go to Step 6
5. To specify access permissions to multiple KVM ports at once for a user or group, do the following:

   a. Select "Multiple Servers" on the "Access List for User - Select the Server" screen.

      The "User Access List – Multiple Servers" screen appears.

   b. Specify the servers using a comma (to separate each server) and/or a hyphen (to specify a range of servers) and press "Enter."

      Valid values include integers only. For example, type "1-6,9" to specify Port_1 through Port_6 and Port_9.

      The "Permission for User: Multiple Servers" screen appears.
6. Select the permissions to be given on the selected port(s).
7. Save the changes.

   The Access List for User - Select the Server screen appears

   The new permissions are indicated by check marks in the appropriate check boxes:

   - r – Read

- w – Write
- p – Power.

8. To reapply the default permissions to a particular user or group, select “Reset All.”

   The following screen appears.

   The system default gives Read and Write permission on all KVM ports.

9. Select “YES” to reset default permissions.

▼ *To Edit Permissions for the Generic User [OSD]*

1. From the User Access List - Select the User screen, select **(Generic Users)** and press <Enter>.
2. Follow the procedures in “To Edit a User or Group’s Access to KVM Ports [OSD]” on page 464.

▼ *To Delete a User From the User Access List [OSD]*

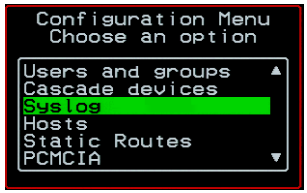
1. Go to Configure>Users and Groups>User Access Lists>Delete User.

   The User Access List - Select the User screen appears.

2. Select the user to delete and press Enter.
3. Select OK on the confirmation screen to return to the main screen.

Configure>Syslog Screens [OSD]

An administrative user can select the Syslog option on the OSD Configuration Menu to specify the IP address for a syslog server.



Selecting the Configure>Syslog option brings up a Server screen for entering the IP address of a syslog server.

To complete the configuration of system logging, you must specify a facility number as shown in “Syslog Facility” on page 390.

See “Configure>Syslog Screens [OSD]” on page 466 for more information.

▼ *To Configure a Syslog Server’s IP Address (OSD)*

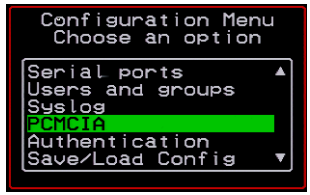
1. Go to: Configure>Syslog.

   The Syslog Sever screen appears.

2. Enter the IP address of the syslog server.
3. Save the changes.

Configure>PCMCIA Screens [OSD]

An administrative user can select the PCMCIA option on the OSD Configuration Menu to configure PCMCIA modem cards. To configure other types of PCMCIA cards, see “Configuration>Network>PCMCIA Management” on page 305



The following diagram lists the screens for configuring PCMCIA modem cards.

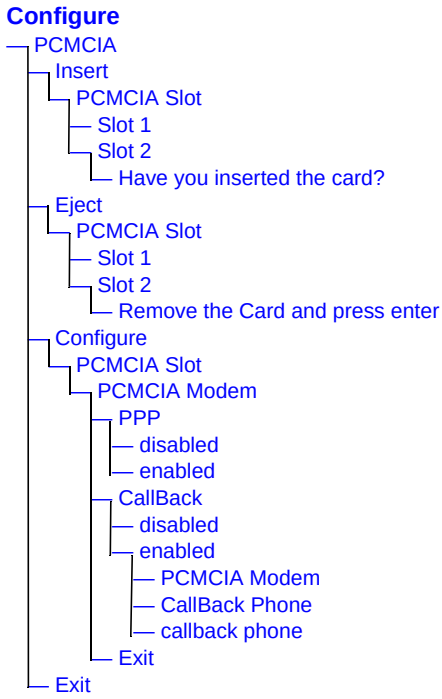
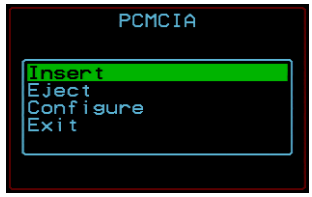
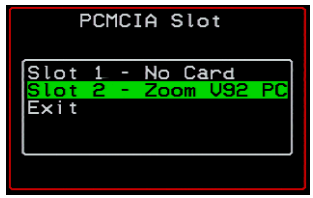


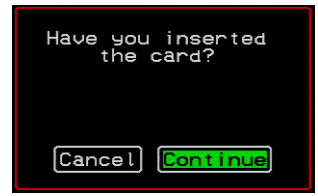
Figure 7-36: OSD Configure>PCMCIA Screens

Selecting the Configure>PCMCIA option brings up a PCMCIA screen with the options shown in the following figure.



When configuring a new card, the administrative user selects the “Insert” option, then select the slot where the new card is inserted. A prompt asks if the card is inserted. The PCMCIA Slot screen and the card insertion query screen are shown in the following figure.





Selecting “Continue,” returns the user to the PCMCIA menu. The OnSite automatically detects the type of card and presents the appropriate series of configuration screens.

The following table shows the screens for a PCMCIA modem card.

Table 7-21: Configuration Screens for a PCMCIA Modem Card [OSD] (Sheet 1 of 3)

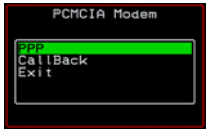
Screen	Description
PCMCIA Modem 	Choices are “PPP,” “CallBack,” or “Exit.”
PPP 	Appears only when PPP is selected from the PCMCIA Modem menu. Options are “disabled” and “enabled.”

Table 7-21: Configuration Screens for a PCMCIA Modem Card [OSD] (Sheet 2 of 3)

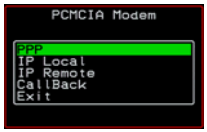
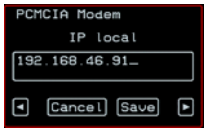
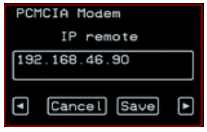
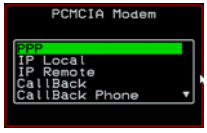
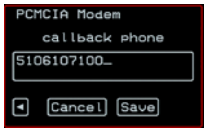
Screen	Description
PCMCIA Modem 	Appears only when PPP is enabled. Choices are: “PPP” for disabling and enabling PPP, “IP Local,” “IP Remote,” “Callback,” and Exit. **Note:** By default, if no local IP is specified, the IP address of the OnSite is used. If no remote IP is specified, the IP address 10.0.0.1 is used. Use the default IP address unless you have a specific reason to use another.
IP Local 	Appears only when PPP is enabled and “IP Local” is selected.
IP Remote 	Appears only when PPP is enabled and “IP Remote” is selected.
callback 	Appears only when “Callback” is selected. Choices are: “disabled” and “enabled.”
PCMCIA Modem 	Appears when callback is enabled with an additional option: “Callback Phone.”

Table 7-21: Configuration Screens for a PCMCIA Modem Card [OSD] (Sheet 3 of 3)

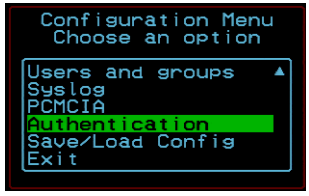
Screen	Description
callback phone 	**Appears only when PPP and callback are enabled and "Callback Phone" is selected from the PCMCIA Modem menu.**

Caution! Before physically ejecting a card, always select the "Eject" option. Ejecting the card without using the Eject option can cause a system panic.

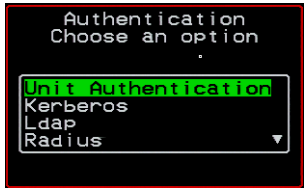
See "Configuring PCMCIA Cards [OSD]" on page 487 for more information.

Configure>Authentication Screens [OSD]

An administrative user can select the Authentication option on the OSD Configuration Menu to configure an authentication method (AuthType) for logins to the OnSite and to configure authentication servers for any type of logins: to the OnSite, to KVM ports, or to serial ports. See "OnSite Authentication Options" on page 7 for details about authentication on the OnSite.



The Authentication menu appears as shown in the following figure.



Not all options are visible.

The following diagram lists the Authentication screens.

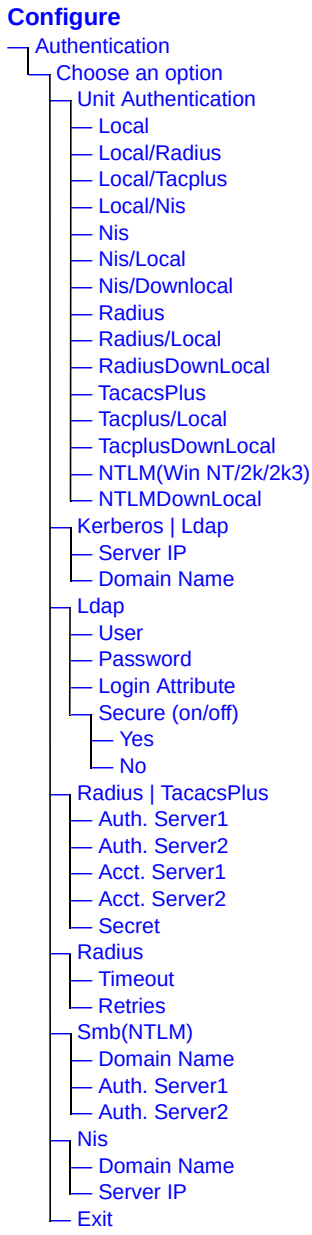
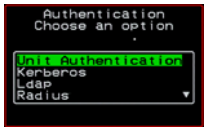
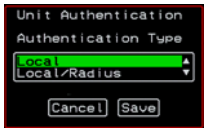


Figure 7-37: OSD Configure>Authentication Options and Screens

The following tables show the screens that appear when the “Authentication” option is selected from the Configure menu in the OSD. The first table shows the screen for choosing an OnSite login authentication method.

Table 7-22: Authentication Configuration Screens for OnSite Logins [OSD]

Screen	Description
Choose an option 	Choose either “Unit authentication” to select an Authentication method for OnSite logins, or choose one of the Authentication methods listed on this screen to configure an authentication server: Kerberos, Ldap, Radius, TacacsPlus, Smb(NTLM), or Nis.
Authentication type 	Authentication method options for OnSite logins. Default = “Local.” Other authorization type options are: Local/Radius, Local/Tacplus, Local/Nis, Nis, Nis/Local, Nis/Downlocal, Radius, Radium/Local, RadiusDownLocal, TacacsPlus, Tacplus/Local, TacplusDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal

The following table shows the common screens that appear when Kerberos or Ldap are selected to configure an authentication server.

Table 7-23: Common Configuration Screens for Kerberos and LDAP Authentication Server [OSD] (Sheet 1 of 2)

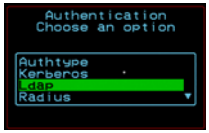
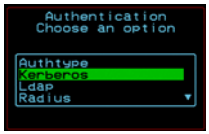
Screen	Description
Ldap 	Choose Ldap to configure an LDAP authentication server.
Kerberos 	Choose Kerberos to configure a Kerberos authentication server.

Table 7-23: Common Configuration Screens for Kerberos and LDAP Authentication Server [OSD] (Sheet 2 of 2)

Screen	Description
Server IP 	IP address of the Kerberos or LDAP server.
Domain Name 	Domain name.

The following table shows the unique screens for configuring an LDAP server, which appear in addition to the screens shown in Table 7-23, “Common Configuration Screens for Kerberos and LDAP Authentication Server [OSD],” on page 472.

Table 7-24: Unique LDAP Authentication Server Configuration Screens [OSD] (Sheet 1 of 2)

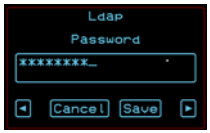
Screen	Description
User 	The LDAP user name.
Password 	The LDAP password.

Table 7-24: Unique LDAP Authentication Server Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
Login Attribute 	The login attribute.
Secure (on/off) 	Choices are “Yes” or “No.”

The following table shows the configuration screens for the Radius and TACACS+ authentication servers.

Table 7-25: Configuration Screens for the Radius or TACACS+ Authentication Servers [OSD] (Sheet 1 of 2)

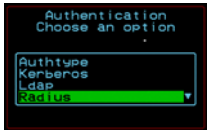
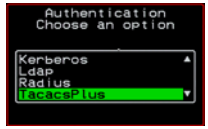
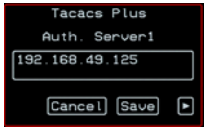
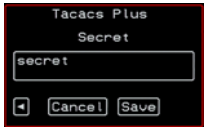
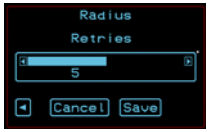
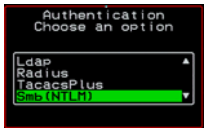
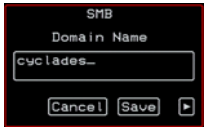
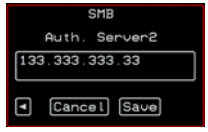
Screen		Description
Radius 	**TacacsPlus** 	Choose Radius or TacacsPlus to configure a Radius or TACACS+ authentication server.
Auth. Server1 	**Auth. Server2** 	IP addresses of one or two authentication servers. The second server is optional.

Table 7-25: Configuration Screens for the Radius or TACACS+ Authentication Servers [OSD] (Sheet 2 of 2)

Screen	Description
Acct. Server1 and Acct. Server2  	IP addresses of one or two optional accounting servers.
Secret 	Shared secret.
Timeout 	Appears only when Radius is selected. Timeout in seconds. Default = 3.
Retries 	Appears only when Radius is selected. Number of retries. Default = 5.

The following table shows the screens for configuring a Smb (NTLM) authentication server.

Table 7-26: Smb (NTLM) Configuration Screens [OSD]

Screen	Description
Smb(NTLM) 	Choose Smb(NTLM) to configure an SMB (NTLM) authentication server.
Domain Name 	The domain name.
Auth. Server1 and Auth. Server2  	IP addresses for one or two SMB (NTLM) authentication servers. The second server IP is optional.

The following table shows the screens for configuring a NIS authentication server.

Table 7-27: NIS Configuration Screens [OSD]

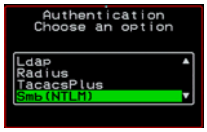
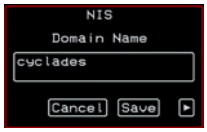
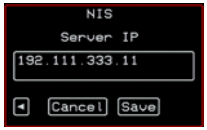
Screen	Description
NIS 	Choose the NIS authentication server.

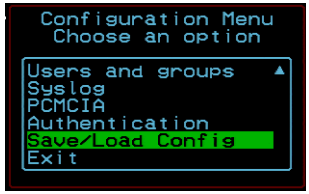
Table 7-27: NIS Configuration Screens [OSD]

Screen	Description
Domain Name 	Enter the Domain Name.
Server IP 	IP address of the NIS server.

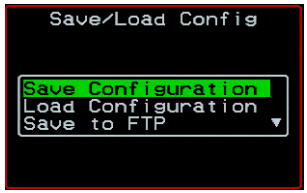
See “Configuring Authentication [OSD]” on page 491 for more information.

Configuration>Save/Load Configuration Screens [OSD]

An administrative user can use the Save/Load Config option on the OSD Configuration Menu to save any configuration changes made since the last save into a backup directory on the OnSite or onto an FTP server. Configuration files from the local backup directory or the remote FTP server can be downloaded to overwrite any configuration changes that were made since the last save. For details about how configuration changes are saved and backed up for possible restoration, see “How Configuration Files Changes Are Managed” on page 574.



The Save/Load Config screen appears as shown in the following figure. Not all menu options are visible.



The following diagram lists the Save/Load Configuration screens.

Configure

- Save/Load Config.
  - Save Configuration
    - Saving configuration . . .
    - Configuration was . . . saved.
  - Load Configuration
    - Restoring configuration . . .
    - Configuration was loaded . . .
  - Save to FTP
    - Save to FTP Server—Filename
    - Server
    - Username
    - Password
    - Saving configuration . . .
    - Configuration was . . . saved
  - Load from FTP
    - Load from FTP Server—Filename
    - Server
    - Username
    - Password
    - Restoring configuration . . .
    - Configuration was loaded . . .
  - Exit

Figure 7-38: OSD Configure>Save/Load Config. Screens

The following table shows the screens that appear when the “Save/Load Configuration” option is selected from the Configure menu in the OSD.

Table 7-28: Save/Load Configuration Screens [OSD] (Sheet 1 of 2)

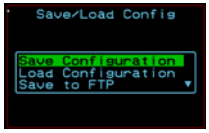
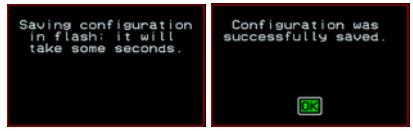
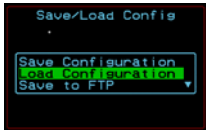
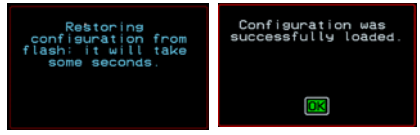
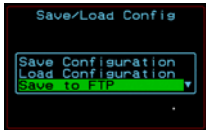
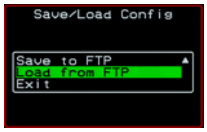
Screen	Description
Save Configuration 	When “Save Configuration” is selected, the following two screens appear. 
Load Configuration 	When “Load Configuration” is selected, the following two screens appear. 
Save to FTP 	When “Save to FTP” is selected, the following five screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.” The last screens confirm the save to FTP succeeded. 

Table 7-28: Save/Load Configuration Screens [OSD] (Sheet 2 of 2)

Screen	Description
Load from FTP 	When “Load from FTP” is selected, the following four screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.” 

See “Configuring the Saving and Restoring of Configuration Files [OSD]” on page 488 for more information.

Configure>Date/Time [OSD]

An administrative user can use the Date/Time screens under Configure>Date/Time to configure the OnSite date and time.

The Date/Time screen allows you to enable or disable an NTP server. If the NTP server is disabled, more screens appear for entering the system date and time manually.

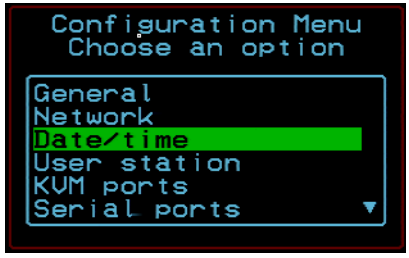


Figure 7-39: Selecting OSD Configure>Date/time

▼ *To Enable the NTP Server to Set the Time and Date [OSD]*

1. From the Main menu of the OSD, go to Configure.

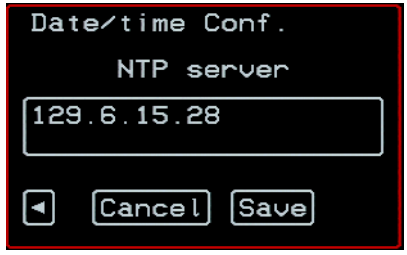
   The Configuration menu appears.

2. Select Date/time.

   The Date/time conf. NTP screen appears.

3. On the NTP screen, select “enabled.”

   The NTP Server screen appears.

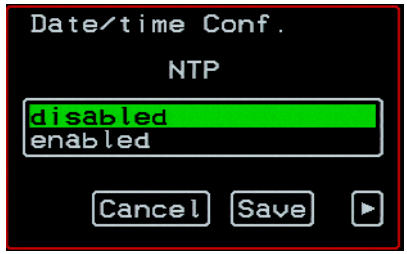


4. Enter the IP address of the NTP server.
5. Save the changes.

▼ *To Enter the Date and Time Manually* [OSD]

1. Go to: Configure>Date/Time>NTP from the OSD Main Menu.

   The NTP screen appears.

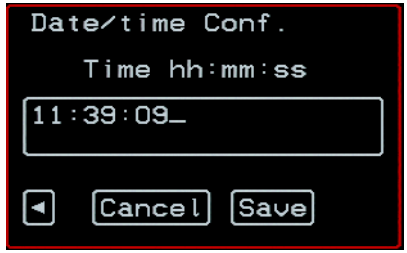


2. On the NTP screen, select “disabled.”

   The Date entry screen appears.

3. Enter the date in YYYY/MM/DD format.

   The Time entry screen appears.



4. Enter the time in hh:mm:ss format.
5. Save the changes.
6. Go to the appropriate menu option for your next task.

Configure>User Station: Power Management Command Key [OSD]

An administrative user can use the Power Management screen under Station Configuration to redefine the command key portion of the KVM power management hot key.

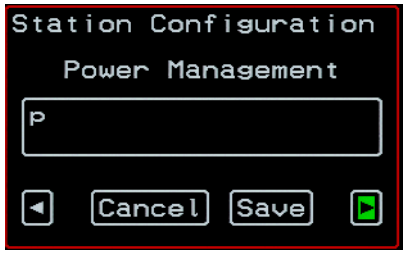


Figure 7-40: Configure>User Station: Power Management Screen

▼ *To Configure the User Station Power Management Command Key* [OSD]

1. Go to Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management.

   The Power Management screen appears.

2. Type the letter to be used for the command key in the power management hot key.

3. Select the next arrow button to go to the Mouse/Keyboard Sync screen.

Configure>User Station: Mouse/Keyboard Reset Command Key [OSD]

An administrative user can use the Mouse/Keyboard Reset screen to redefine the command key portion of the mouse/keyboard reset hot key.

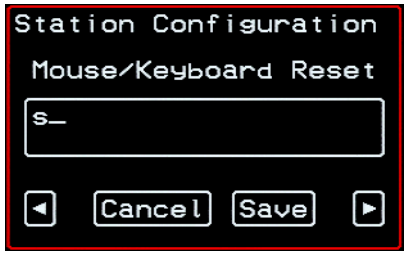


Figure 7-41: Configure>User Station: Mouse/Keyboard Reset Screen

▼ *To Specify the User Station Mouse/Keyboard Reset Command Key* [OSD]

1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management>Mouse/Keyboard Sync.

   The Mouse/Keyboard Sync screen appears.

2. Type the letter to be used for the command key in the mouse/keyboard sync hot key.
3. Select the next arrow button to go to the Video Configuration screen.

Configure>User Station: Video Configuration Command Key [OSD]

An administrative user can use the Video Configuration screen to redefine the command key portion of the video configuration hot key.

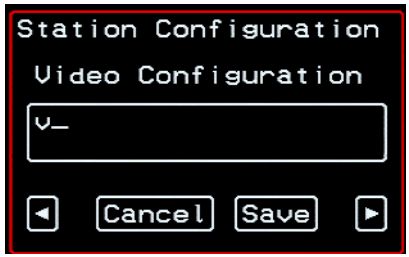


Figure 7-42: Configure>User Station: Mouse/Keyboard Reset Screen

▼ *To Specify the User Station Video Configuration Command Key* [OSD]

1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management>Mouse/Keyboard Sync>Video Configuration.

   The Video Configuration screen appears.

2. Type the last letter of the mouse/keyboard sync keyboard shortcut.
3. Select the next arrow button to go to the Switch Next screen.

Configure>User Station: Switch Next Command Key [OSD]

An administrative user can use the Switch Next screen to redefine the command key portion of the “Switch Next” keyboard shortcut.

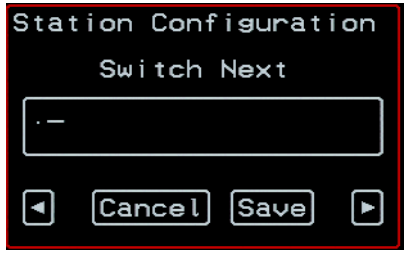


Figure 7-43: Configure>User Station: Switch Next Screen

▼ *To Specify the User Station Switch Next Command Key* [OSD]

1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management>Mouse/Keyboard Sync>Video Configuration>Switch Next.

   The Switch Next screen appears.

2. Type the last letter of the switch next keyboard shortcut.
3. Select the next arrow button to go to the Switch Previous screen.

Configure>User Station: Switch Previous Command Key [OSD]

An administrative user can use the Switch Previous screen to define Command Key portion of the switch previous keyboard shortcut.

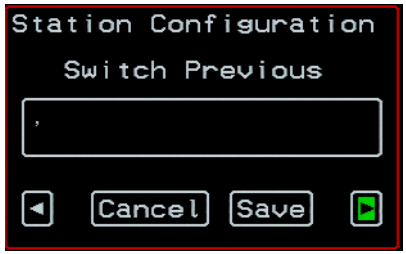


Figure 7-44: Configure>User Station: Switch Previous Screen

▼ *To Specify the User Station Switch Previous Command Key* [OSD]

1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management>Mouse/Keyboard Sync>Video Configuration>Switch Next>Switch Previous.

   The Switch Previous screen appears.

2. Type the last letter of the switch previous keyboard shortcut.
3. Select the next arrow button to go to the Port Info screen.

Configure>User Station: Port Info Command Key [OSD]

An administrative user can use the Port Info screen to define the Command Key portion of the port info keyboard shortcut.

Figure 7-45: Configure>User Station: Port Info Screen

▼ *To Specify the Keys Used in the Command Key Portion of the Port Info Keyboard Shortcut* [OSD]

1. Go to: Configure>User Station>Idle Timeout>Screen Saver Time>Cycle Time>Keyboard Type>Quit>Power Management>Mouse/Keyboard Sync>Video Configuration>Switch Next>Switch Previous>Port Info.

   The Port Info screen appears.

2. Type the last letter of the port info keyboard shortcut.
3. Select Save to save your configuration.

Configuring PCMCIA Cards [OSD]

An administrative user can use the PCMCIA screen to configure an installed and configured modem card. You can allow a user to call in through PPP or enable callback.

▼ *To Configure a PCMCIA Card* [OSD]

1. Go to Configure>PCMCIA.

   The “Slot” screen appears.

2. Select the slot (slot 1 or slot 2) where the PCMCIA card is installed.

   The “PPP” screen appears.

3. Select one of the following:

   - To enable PPP, select the “enabled” option and go to Step 4

     The “IP Local” screen appears.

- To disable PPP, select the “disabled” option and go to Step 6
  The “callback” screen appears.

4. On the “IP local” screen, specify the local IP address.

   The “IP remote” screen appears.

5. On the “IP remote” screen, specify the remote IP address.

   The “Callback” screen appears.

6. On the “Callback” screen, do one of the following:
   - To disable callback, select the “disabled” option.
     If callback is disabled, this is the last step.
   - To enable callback, select the “enabled” option and go to Step 7
     The “callback phone” screen appears.

7. If callback is enabled, enter a callback phone number.

Configuring the Saving and Restoring of Configuration Files [OSD]

An administrative user can use the Save/Load Config menu options to save the configuration to flash and to upload or download the configuration file to or from an FTP server.

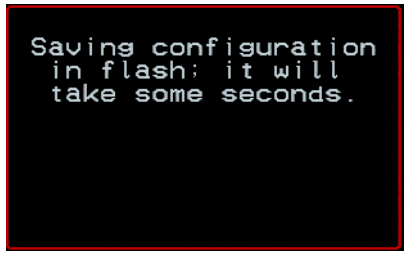
▼ *To Save Configuration Files to Flash* [OSD]

1. Go to: Configure>Save/Load Config.

   The “Save/Load Config” screen appears.

2. Select “Save Configuration.”

   The following two messages appear.



3. Select OK to complete the procedure.

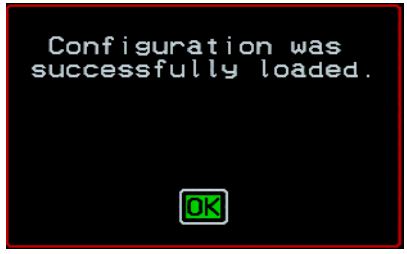
▼ *To Load The Configuration File from Flash* [OSD]

1. Go to: Configure>Save/Load Config.

   The Save/Load Config screen appears.

2. Select “Load Configuration.”

   The following message appears.



3. Select OK to complete the procedure.

▼ *To Save Configuration Files to an FTP Server* [OSD]

1. Go to Configure>Save/Load Config.

   The “Save/Load Config” screen appears.

2. Select “Save to FTP.”

   The “Save to FTP Server – Filename” screen appears.

3. Enter the name of the configuration file.

   The “Server” screen appears.

4. Enter the name of the FTP server.

   The “Username” screen appears.

5. Enter the username used to access the FTP Server.

   The “Password” screen appears.

6. Type the password used to access the FTP server.

7. Select “Save” to complete the procedure.

▼ *To Load Configuration Files from an FTP Server* [OSD]

1. Go to: Configure>Save/Load Config.

   The “Save/Load Config” screen appears.

2. Select “Load from FTP.”

   The “Load from FTP Server – Filename” screen appears.

3. Enter the name of the configuration file.

   The “Server” screen appears.

4. Enter the name of the FTP server.

   The “Load from FTP Server – Username” screen appears.

5. Enter the username of the account used to access the FTP server.

   The “Password” screen appears.

6. Type the password used to access the FTP server.
7. Select Save to restore the configuration.

Configuring Authentication [OSD]

An administrative user can use the “Authentication” option under Configuration in the OSD to specify an authentication method for the OnSite (under “Unit Authetication) and to configure authentication servers. You need to identify an authentication server for each authentication method specified for the OnSite, for direct logins to KVM ports, or for logins to serial ports. The authentication servers must be fully configured and available for the OnSite to access over the network. Work with the system administrator of the authentication server to obtain the information you need to enter on the authentication screens.

▼ *To Configure an Authentication Method and an Authentication Server for OnSite Logins* [OSD]

1. Go to: Configure>Authentication.

   The “Authentication” screen appears.

2. Select “Unit Authentication.”

   The “Authentication Type” screen appears.

3. Select the authentication method to use.

   See “Choosing Among Authentication Methods” on page 7 for an explanation of each method.

   The “Authentication” screen appears.

4. Configure the authentication parameters for the selected type.

See Table 7-29 for a list of tasks for configuring authentication servers and where to find the tasks are documented.

Table 7-29: Tasks for Configuring Authentication Servers

Authentication Type	Where Documented
Kerberos, Local/Kerberos, Kerberos/Local, or KerberosDownLocal	"To Configure a Kerberos Authentication Server [OSD]" on page 492
LDAP, Local/LDAP, LDAP/Local, or LDAPADownLocal	"To Configure an LDAP Authentication Server [OSD]" on page 494
RADIUS, Local/RADIUS, RADIUS/Local, or RADIUSDownLocal	"To Configure a RADIUS Authentication Server [OSD]" on page 496
TACACSPlus, Local/TACACSPlus, TACACSPlus/Local, or TACACSPlusDownLocal	"To Configure a TACACS+ Authentication Server [OSD]" on page 496
SMB	"To Configure an SMB Authentication Server [OSD]" on page 497
NIS, Local/NIS, NIS/Local, or NISDownLocal	"To Configure an NIS Authentication Server [OSD]" on page 497

▼ *To Configure a Kerberos Authentication Server* [OSD]

Perform the following to identify the authentication server when the OnSite or any of its ports is configured to use either the Kerberos, Local/Kerberos, Kerberos/Local, or KerberosDownLocal authentication method.

Before starting this procedure, find out the following information from the Kerberos server's administrator:

- Realm name and KDC address
- Host name and IP address for the Kerberos server

Work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If Kerberos authentication is specified for the OnSite, accounts for all users who need to log into the OnSite to administer connected devices.

1. Make sure an entry for the OnSite and the Kerberos server exist in the OnSite's `/etc/hosts` file.

a. Go to: Configure>Hosts>Edit.

The Select a Hosts screen appears.

b. Scroll the list of servers to verify whether an entry exists. If an entry exists, go Step 2.

c. Add an entry for OnSite if none exists and an entry for the Kerberos server.

See "To Edit a Host [OSD]" on page 419 for the instructions for adding a host.

2. Make sure that timezone and time and date settings are synchronized on the OnSite and on the Kerberos server.

Time and date synchronization is most easily achieved by setting both to use the same NTP server. See "To Enable the NTP Server to Set the Time and Date [OSD]" on page 481 for details about how to use the OSD to specify an NTP server.

a. Go to Expert>Configuration>Network>Time/Date.

3. If the OnSite is not located in the PST time zone, set the timezone on the OnSite.

a. Make a console connection to the OnSite and log in as root,

```
AlterPath OnSite login: root
Password: ********
```

The root prompt appears,

```
[root@onsite root]#
```

b. Enter **set_timezone**.

A list of timezones appears followed by a prompt asking you to enter a number of a timezone.

```
[root@kvmnet root]# set_timezone
Please choose the time zone where this machine is located.
 1) Africa       18) Eire         35) Jamaica      52) ROC
...
17) Egypt        34) Israel       51) Portugal     68) zone.tab
Enter the number corresponding to your choice:
```

c. Enter the number of the timezone where the OnSite is located.

```
Enter the number corresponding to your choice: EDT
```

d. Logout from the console session and close the terminal.

4. In the OSD, go to Configure>Authentication.
5. Select Kerberos.

   The “Kerberos Server IP” screen appears.
6. Enter the information in the screens according to the setup of the Kerberos server.
7. Save the changes when you are finished entering information in the last Kerberos screen.

▼ *To Configure an LDAP Authentication Server [OSD]*

Perform the following to configure the authentication server when the OnSite or any of its ports is set up to use either the LDAP, Local/LDAP, LDAP/Local, or LDAP/Down Local authentication method. Before starting this procedure, find out the following information from the LDAP server’s administrator:

- The distinguished name of the search base
- The LDAP domain name
- Whether to use secure LDAP
- The server’s IP address

An administrative user can enter information in the following two fields, but an entry is not required:

- The LDAP password
- The LDAP user name

Work with the LDAP server's administrator to ensure that the following types of accounts are set up on the LDAP server and that the administrators of the OnSite and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If LDAP authentication is specified for the OnSite, accounts for all users who need to log in to the OnSite to administer connected devices.
- If LDAP authentication is specified for KVM ports, accounts For users who need administrative access all administrative users (won't they need to be root users?)

1. In the OSD, go to Configure>Authentication.
2. Select LDAP.

   The LDAP Server IP screen appears with the field filled in from the current value in the `/etc/ldap.conf` file.
3. Supply the IP address of the LDAP server in the LDAP Server IP field and press Enter.

   The LDAP Domain Name (Search base) screen appears with field filled in from the current value in the `/etc/ldap.conf` file.
4. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the LDAP Domain Name field, change the base definition.

   The default distinguished name is "dc," as in `dc=`*`value`*`,dc=`*`value`*. If the distinguished name on the LDAP server is "o," then replace `dc` in the base field with `o`, as in `o=`*`value`*`,o=`*`value`*`.`
5. Replace the default base name with the name of your LDAP domain.

   For example, for the LDAP domain name cyclades.com, the correct entry is: `dc=cyclades,dc=com`.
6. Fill in the other screens according to your local setup of the LDAP server.
7. Click Save once you are done with the last screen.

The changes are stored in `/etc/ldap.conf` on the OnSite.

▼ *To Configure a RADIUS Authentication Server* [OSD]

Perform the following when the OnSite or any of its ports is configured to use either the RADIUS, Local/RADIUS, RADIUS/Local, or RADIUSDownLocal authentication methods.

1. Go to Configure>Authentication.
2. Select RADIUS.

   The first RADIUS screen appears.
3. Fill in each screen according to your local setup of the RADIUS server or servers.
4. Select Save.

   The changes are stored in `/etc/raddb/server` on the OnSite.

▼ *To Configure a TACACS+ Authentication Server* [OSD]

Perform the following to identify the authentication server when the switch or any of its ports is configured to use either the TACACSPlus, Local/TACACSPlus, TACACSPlus/Local, or TACACSPlusDownLocal authentication method.

1. In the OSD, go to Configure>Authentication.
2. Select TACACSPlus.

   The first TACACSPlus screen appears.
3. Fill in the screens according to your local setup of the TACACSPlus server.
4. Click Save once you are done with the last screen.

   The changes are stored in `/etc/tacplus.conf` on the switch.

▼ *To Configure an SMB Authentication Server* [OSD]

Perform the following to identify the authentication server if any of the ports is configured to use the SMB authentication method.

1. In the OSD, go to Configure>Authentication.
2. Select SMB.

   The first SMB screen appears.
3. Fill in the screens according to your local setup of the SMB server.
4. Click Save once you are done with the last screen.

▼ *To Configure an NIS Authentication Server* [OSD]

Perform the following to identify the authentication server when the switch or any of its ports is configured to use either the NIS, Local/NIS, NIS/Local, or NISDownLocal authentication method.

1. In the OSD, go to Configure>Authentication.
2. Select NIS.

   The first NIS screen appears.
3. Fill in the screens according to your local setup of the NIS server.
4. Click Save once you are done with the last screen.

System Info Menu [OSD]

An administrative user can choose the System Info option on the OSD Main Menu to view detailed information about the OnSite.

The following table shows the type of information displayed on the System Info screen.

Table 7-30: System Information Example [OSD]

Information Type	Example
BOARD	OnSite
	Serial ports: 8
	KVM ports: 8
	User stations: 2
	ID: 8cfb990b0000
Version (Software)	Firmware: 1.1.0
	SYS FPGA: 0xb3/2
MEMORY	RAM: 124 Mbytes
	RAM usage: 22%
	Flash: 248 MB
CPU	Clock: 130 MHz
DAT/TIME	Sat 06 May 2006
	17:05:10 GMT up 1 day, 2:41
USER1 CONNECTION	Int. uC, V1.1.0
USER2 CONNECTION	None

▼ *To Access System Information* [OSD]

1. On the Main Menu, select System Info.

   The System Info screen appears.

2. Use the up and down arrow keys to view the information.
3. To exit, press the escape key.

Reboot [OSD]

An administrative user can choose the Reboot option on the OSD Main Menu to reboot the OnSite.

▼ *To Reboot the OnSite*

1. Select Reboot from the Main Menu.

   The configuration dialog appears.

2. Select Yes to reboot the OnSite.

Chapter 8
Miscellaneous Procedures

This chapter describes how to perform configuration procedures that cannot be performed using the Web Manager.

Disabling or Modifying Inactivity Timeouts

An inactivity timeout period is set in the Web Manager for security. An administrator who knows the root password and can log into the OnSite console can change the timeout value, if desired, by editing a line in the `webui.conf` file, as described in the following procedure.

▼ *To Disable Web Manager Timeouts*

This procedure can be performed by an administrator who knows the root password and can log into the OnSite console.

1. From a terminal or terminal emulation application, log into the OnSite console as root.

```
OnSite login: root
Password: root_password
```

2. Open the `/etc/daemon.d/webui.conf` file for editing.
3. Find the line that begins with `DPARM`.

   The default line is shown in the following screen example.

```
DPARM="$HTTP_PORT $HTTPS_PORT $SECLEVEL $SSLVER"
```

4. Add the `-T` *n* option to set a timeout value of *n*.

   The `-T 0` setting shown in the following screen example sets the timeout to zero (0).

```
DPARM="-T 0 $HTTP_PORT $HTTPS_PORT $SECLEVEL $SSLVER"
```

5. Stop and restart the web server to put the certificate into effect.

```
[root@OnSite /root]# daemon.sh stop WEB
[root@OnSite /root]# daemon.sh restart WEB
```

OTP Configuration

As introduced in “One Time Password Authentication on the OnSite” on page 18, *OPIE* (*one-time passwords in everything*) software on the OnSite supports the *one-time password* (OTP) authentication method for some types of access.

As shown in Table 1-3 on page 9, the OTP authentication method and the OTP/Local fallback option are supported for serial ports, and the OTP authentication method is supported for dial-ins through modem, GSM, and CDMA PCMCIA cards.

Note: OTP authentication is not supported for logins to the OnSite or to KVM ports.

This section describes what the OnSite administrator must do to configure OTP authentication.

OnSite administrators must perform OTP configuration tasks in the order given in the following bulleted list:

- The OnSite root user manually enables OTP and configures where to mount the OPIE databases.
- An OnSite administrative user may also use the Web Manager or `CLI` to configure OTP authentication to be used for dial-ins to modem, GSM, and CDMA PCMCIA cards.
- An OnSite administrative user may also use the Web Manager, OSD, or `CLI` to configure OTP or OTP/Local authentication methods for serial port logins or serial port dial-ins, when a modem is connected to a serial port configured for PPP access.
- An OnSite administrator must make sure each user who needs to use OTP has a local account on the OnSite, is registered with the OTP system, and is able to obtain the OTP passwords, OTP username, and secret pass phrase needed for login.

The following table lists the OTP authentication configuration tasks and where they are documented.

Table 8-1: Tasks for Configuring OTP Authentication

Task	Where Documented
Edit the `/etc/otp.conf` file to configure the location used for storage of OPIE databases.	"Editing the otp.conf File" on page 506
Run the `/bin/do_create_otpdb` script to initialize OTP and mount the directory to be used for OPIE database storage.	"To Specify the Location for the OTP Databases" on page 507
Configure OTP or OTP/Local as the authentication method for access to all serial ports or individual serial ports.	Web Manager: "To Configure a Serial Port Authentication Method [Expert]" on page 241 OSD:"To Specify an Authentication Method for Serial Ports [OSD]" on page 450 CLI: `cli> config physicalports` [specify "all" or a port number from 1-8] `access authtype [otp | otplocal]`
Configure OTP authentication for dial-ins through PCMCIA modem, GSM, and CDMA cards.	Web Manager: "Configuring a Modem PCMCIA Card" on page 307, "Configuring a GSM PCMCIA Card" on page 311, "Configuring a CDMA PCMCIA Card" on page 316 OSD: "To Configure a PCMCIA Card [OSD]" on page 487 CLI: `cli> config network pcmcia` [specify a slot number "1" or "2"] [specify `modem | cdma | gsm`] `otpauthreq`

Table 8-1: Tasks for Configuring OTP Authentication (Continued)

Task	Where Documented
Make sure each user who needs to use OTP has a local user account, is registered with the OTP system, and is able to obtain the OTP username, OTP secret pass phrase, and OTP passwords needed for logins. See the following list for options:	"How Users are Registered with OTP and Obtain OTP Passwords" on page 509
• Register each user yourself and give the OTP username and OTP secret pass phrase to each user.	"To Register and Generate OTP Passwords for Users" on page 510
• Generate the needed OTP passwords on behalf of the each user and give them to each user.	
• Make sure users are equipped with an OTP generator that is not on the network to generate their own OTP passwords when challenged at login time.	Example: • User dials into the OnSite through a PCMCIA modem card that has been configured to use OTP authentication. • OnSite challenges with the sequence number and seed associated with the username and asks for a response. • User enters the sequence number, seed, and the secret pass phrase locally into a copy of `opiekey` on the user's laptop and obtains an OTP password. • User answers the OnSite challenge with the OTP password and gets dial-in access to the OnSite.

For more details about OTP, see: `http://www.freebsd.org/doc/en/books/handbook/one-time-passwords.html`.

Editing the otp.conf File

OTP expects its user databases to reside in `/mnt/opie/etc`. The OnSite administrator must edit the `/etc/otp.conf` file to configure a location for the OTP databases by configuring where `/mnt/opie` is to be mounted.

The following table lists the devices that may be used for mounting `/mnt/opie` and the keywords and values used to identify each type of device in the `otp.conf` file, and it provides additional information in the "Notes" column.

Table 8-2: Devices Available for Mounting OPIE Databases

Location Option	Keyword or Accepted Value	Notes
Local filesystem	LOCAL	The filesystem must be in the OnSite's resident flash memory.
Compact flash PCMCIA card	PCMCIA	A compact flash PCMCIA card must be installed and configured. The values assigned PCMCIA/CF, FSTYPE and MOUNTPT from `ide.opts` are used.
NFS-mounted directory	*host*:*path*	*host* must be the DNS name or IP address for the NFS server. *path* must be the path to an directory shared (exported) by the NFS server.

▼ To Specify the Location for the OTP Databases

1. Log in to the OnSite's console as root.
2. Change to the `/etc` directory and use a text editor to open the `otp.conf` file for editing.

```
[root@OnSite /]# cd /etc
[root@OnSite /]# vi otp.conf
#
# ENABLE can be 'YES' or 'NO'
#
ENABLE=NO
#
# Where to mount the otp database
#
MOUNT_POINT=/mnt/opie
#
# Device specify where otp database will be. it can be:
#
#   LOCAL     - should be used only if FS is in the builtin
IDE/CF
#   PCMCIA    - PCMCIA/CF, FSTYPE and MOUNTPT from ide.opts
will be used
#   host:path - NFS
#
DEVICE=PCMCIA
```

3. Set `ENABLE=YES`.

```
# ENABLE can be 'YES' or 'NO'
#
ENABLE=YES
```

4. Specify the device where the OTP databases are to be stored.

   See Table 8-2 for the accepted values for `DEVICE`. The following screen example shows specifying an NFS server named

exodus.cyclades.com and the path to a /home/opie directory on the NFS server.

```
DEVICE=exodus.cyclades.com:/home/opie
```

5. Save and quit the file.

```
:wq
```

6. Do the procedure under"To Enable OTP and Configure the Location for OTP Databases" on page 508.

Running the /bin/do_create_otpdb Script

After editing the /etc/otp.conf file, the root user needs to log in locally through the OnSite's console port and run the /bin/do_create_otpdb script on the command line. The script does the following:

- Enables OTP
- Mounts the location (PCMCIA, local directory, or NFS-mounted directory) specified in the otp.conf file onto the /mnt/opie directory
- Creates the directory /mnt/opie/etc
- Creates the file /mnt/opie/etc/opiekeys
- Sets the permissions of the file to mode 0644, the owner of file to "root," and the group to "bin"
- Creates the directory /mnt/opie/etc/opielocks for the OPIE lock files
- Sets the permissions of this directory to 0700 and the owner and group to "root"

▼ To Enable OTP and Configure the Location for OTP Databases

Do this procedure after "To Specify the Location for the OTP Databases" on page 507.

1. Log in locally through the OnSite's console port as root.
2. Run the /bin/do_create_otpdb script on the command line.

3. Perform the procedure under"To Register and Generate OTP Passwords for Users" on page 510.

How Users are Registered with OTP and Obtain OTP Passwords

All users who need to use OTP authentication must have a local account on the OnSite, must be registered with the OTP system, and must be able to obtain OTP passwords.

The OPIE commands in the following bulleted list must be executed with the `-c` option while a user is logged in locally through the OnSite's console port.

- The `opiepasswd` command to register users
- The `opiekey` command to generate OTP passwords

The requirement for local logins through the console port is enforced for regular users because running the commands through a dial-up or other insecure connection can expose the user passwords, pass phrases, and OTP passwords. The root user can execute these commands without the `-c` option while logged in over `ssh` because `ssh` provides a secure path. The OPIE commands should never be executed over a dial-up connection.

OTP passwords are generated in one of the two following ways:

- By the user or administrator executing the `opiekey` command

  If the `opiekey` command is executed by an administrator on behalf of a user, the administrator must provide the username and the secret pass phrase that were used to register the user to the user along with the generated OTP passwords.

- By the user with a password generating device (more likely scenario)

  If a user has a password generating device, then the user generates the OTP password when challenged at login using the username and secret pass phrase, along with the seed and sequence number (the seed and sequence number are displayed along with the OTP challenge).

The following procedure shows an example of an administrator logging in locally through the console port, registering a user, and generating OTP passwords for the user. The example shows running the `adduser` command to add the user, but any of the tools available for adding users, including the Web Manager, may be used to configure the user account beforehand.

▼ To Register and Generate OTP Passwords for Users

Do this procedure for each user who needs to use OTP authentication after "To Enable OTP and Configure the Location for OTP Databases" on page 508.

1. Log in locally through the OnSite's Console port as root or use `ssh` to log into the OnSite's console.
2. Make sure each user authorized for dial-ins has a local account on the OnSite.

Note: You can separately use the Web Manager to add users instead of doing this step.

For example, the following screen shows using the `adduser` command to add user `joe` and set the user's password to "`joes_passwd`."

```
[root@OnSite /]# adduser joe
New password: joes_passwd
Re-enter new password: joes_passwd
Password changed
```

3. Enter the `opiepasswd` command to register the user.

   The following screen example shows using `opiepasswd` with the `-c` option while logged in locally through the OnSite's CONSOLE port. If you are logged into the OnSite's console using `ssh`, do not use the `-c` option.

   The example shows using "`joe`" as the username and "`joes secret pass phrase`" as the secret pass phrase.

Note: The secret pass phrase is not the same as the user's regular login password.

In the example, the `opiepasswd` command generates a default OPIE sequence number of `499` and a creates a key from the first two letters of the hostname and a pseudo random number, in the example `ON93564`.

```
[root@OnSite /]# opiepasswd -c joe
Adding joe
Reminder - Only use this method from the console; NEVER from
remote. If you are using telnet, xterm, or a dial-in, type ^C
now or exit with no password. Then run opiepasswd without the
-c parameter. Using MD5 to compute responses.
Enter new secret pass phrase: joes secret pass phrase
Again new secret pass phrase: joes secret pass phrase

ID joe OPIE key is 499 ON93564
CITY MARY GLOW ZION MAY ARM
[root@OnSite /]#
```

4. If needed, enter the `opiekey` command with the `-c` option to generate a number of passwords and supply them to the user.

   The following command line example uses the `-n 5` option followed by the 498 to generate 5 passwords ending with sequence number 498.

```
[root@OnSite /]# opiekey -n 5 498 CA93564 -c
Using MD5 algorithm to compute responses.
Enter secret pass phrase: joes secret pass phrase
494: WORD ROW GIFT NET BLUE MOM
495: AMEN FONT STAR SEA WINE RED
496: ART LILY HOLY AID LOVE ALL
497: GOLD ARK FISH DOVE SON ZION
498: SEE PITY JOY HOPE PLAN CITY
[root@OnSite /]#
```

5. Give the OTP username, secret pass phrase, and any OTP passwords generated in this procedure to the user.

Configuring Groups on LDAP, NTLM, RADIUS, and TACACS+ Authentication Servers

This section describes how to configure groups on LDAP, NTLM, RADIUS, and TACACS+ authentication servers and perform the required configuration on the OnSite to support group authorizations for these authentication methods.

On the OnSite, the users and groups must be defined with the same names used in the authentication servers. See the user configuration procedures under Table 1-8, "Tasks for Configuring Users," on page 22.

Configuring Groups for TACACS+

The following list defines the values that must be defined when configuring a group with TACACS+ authentication.

- The TACACS+ administrator must add each user to a group. To give a user administrative access, the user must be added to the `admin` group.
- On the OnSite, the TACACS+ authentication server must be configured for raw access, in either of the two ways shown in the following table:

Method	Procedure
Web Manager	Follow the procedure in "To Configure a TACACS+ Authentication Server [Expert]" on page 286, making sure to check the "Enable Raccess Authorization" checkbox.
OnSite Command Line	"Configuring a TACACS+ Authentication Server on the Command Line" on page 513

▼ *To Configure Groups for TACACS+*

Perform this procedure by editing the AA database on the TACACS+ server. These additions can be made through a GUI. The example shows a declaration that would need to be added to the AA database if a GUI is not available.

- Add the `raccess` service to each user's configuration and define the `group_name` to which each user belongs.To give a user administrative access, make the `group_name = admin`.

```
user = username {
     global = cleartext "group password"  {

     service = raccess  {
       group_name = groupname;
     }
}
```

Configuring a TACACS+ Authentication Server on the Command Line

The following list defines the values that must be defined when configuring a TACACS+ authentication server.

- *authhost1:* IP address of the TACACS+ authentication server. A second TACACS+ authentication server can be configured with the parameter *authhost2*.
- *accthost1:* IP address of a TACACS+ accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not defined, accounting is not be performed. If the same server is used for authentication and accounting, both parameters must be defined with the same address. A second TACACS+ accounting server can be configured with the parameter *accthost2*.
- `secret`: The shared secret (password) necessary for communication between the OnSite and the TACACS+ servers.
- `encrypt`: The default is 1, enable encryption. 0 means disable encryption.
- `service`: The service to be enabled, in this case: "raccess."
- `protocol`: The default is `lcp` (line control protocol). Specify another parameter if required.

- `timeout`: The timeout (in seconds) for a TACACS+ authentication query to be answered.
- `retries`: Defines the number of times a TACACS+ server is tried before another is contacted. The first server authhost1 is tried for the specified number of times, before the second authhost2, if configured, is contacted and tried for the specified number of times. If the second server fails to respond or if no second server is configured, TACACS+ authentication fails.

▼ To Configure a TACACS+ Authentication Server on the Command Line

1. On the OnSite, edit the following parameters in the `/etc/tacplus.conf` file, changing the values as described under "Configuring a TACACS+ Authentication Server on the Command Line" on page 513.

```
authhost1=TACACS+_authentication_server_IP
accthost1=TACACS+_accounting_server_IP
secret=secret
encrypt=1
service=raccess
protocol=lcp
timeout=10
retries=2
```

Note: If configuring group access on the TACACS+ authentication server, `service` must be defined as `raccess`.

2. Save and quit the file.

Configuring Groups for RADIUS

The following list defines the values that to define when configuring a RADIUS authentication server on the OnSite.

- `auth1` server[:port] secret [timeout] [retries]
- `acct1` server[:port] secret [timeout] [retries]

where:

- `auth1`: The first RADIUS authentication server.
- `acct1`: The first RADIUS accounting server.
- *server*: The RADIUS server address.
- *port*: Optional. The default port name is “radius” and is looked up through `/etc/services`.
- *secret:* The shared password required for communication between the OnSite and the RADIUS server.
- *retries:* The number of times each RADIUS server is tried before another is contacted.
- *timeout:* The default is 3 seconds. How long the authentication server should wait before sending a success or failure response.

▼ To Configure Groups for RADIUS

1. On the RADIUS server, open the `/etc/raddb/users` file for editing.
2. Assign groups to a user in a new string attribute (Framed-Filter-Id) similar to the following example.

```
groupuser1
Auth-Type= Local, Password =”xxxx”
         Service-Type=Callback-Framed-User,
         Callback-Number=”305”,
         Framed-Protocol=PPP,
         Framed-Filter-
         Id=”:group_name=<Group1>[,<Group2>,...,<GroupN>]”,
         Fall-Through=No
```

Note: If the Frame-Filter-Id already exist, append the `group_name` declaration to the string starting with a colon “:”

---

3. Save and quit the file.

Configuring a RADIUS Authentication Server on the Command Line

The following list defines the values that to define when configuring a RADIUS authentication server on the OnSite.

- `auth1` *`server`*[`:`*`port`*] *`secret`* [*`timeout`*] [*`retries`*]
- `acct1` *`server`*[:*`port`*] *`secret`* [*`timeout`*] [*`retries`*]

where:

- `auth1`: The first RADIUS authentication server.
- `acct1`: The first RADIUS accounting server.
- *`server`*: The RADIUS server IP address.
- *`port`*: Optional. The default port name is “radius” and is looked up through `/etc/services`.
- *`secret:`* The shared password required for communication between the OnSite and the RADIUS server.
- *`timeout:`* How long the authentication server should wait before sending a success or failure response. The default is 3 seconds.
- *`retries:`* The number of times the RADIUS server is tried before the second defined RADIUS server is contacted. The default is 2.

▼ To Configure a RADIUS Authentication Server on the Command Line

1. On the OnSite, open the `/etc/raddb/server` file for editing.
2. Make an entry for the RADIUS server (`auth1`), an accounting server (`acct1`), and if desired, make an entry for a second RADIUS authentication server (`auth2`) and for a second accounting server (`acct2`), by performing the following steps for each server.
   a. Enter the IP address for the server.
   b. Optional: define an alternate port.
   c. Enter the secret (shared password.
   d. Optional: enter a value to redefine the timeout.
   e. Optional: enter a value to redefine the number of retries.

The following screen example shows entries that define the RADIUS authentication server and the accounting server to be the same server with the same IP address, sets the *secret* to cyclades, the *timeout* to 5 seconds, and the number of *retries* to 5.

```
auth1 172.20.0.2 cyclades 5 5
acct1 172.20.0.2 cyclades 5 5
```

Note: Always configure both parameters `auth1` and `acct1`.

3. Save and quit the file.

Multiple RADIUS servers can be configured in this file. The servers are tried in the order in which they appear. If a server fails to respond, the next configured server is tried.

▼ To Configure User or Group Authorization for Accessing Serial Ports [CLI]

1. Log into the OnSite console and bring up the `CLI` utility.
2. Enter the parameters shown in the following screen example, followed by a comma-separated list of usernames or groupnames.

```
cli > config physicalports serial_port_number access
users/groups comma-separated_list_of_usernames_or_groupnames
```

3. Save the changes.

```
cli > config savetoflash
```

Configuring Groups for LDAP

1. On the server, edit the “info” attribute for the user and add the following syntax.

```
info: group_name=<Group1>[,<Group2>,...,<GroupN>];
```

2. On the OnSite, configure groups to access the serial ports.

a. Log into the OnSite console and bring up the `CLI` utility.

b. Enter the parameters shown in the following screen example, followed by a comma-separated list of usernames or groupnames.

```
cli > config physicalports serial_port_number access
users/groups comma-separated_list_of_usernames_or_groupnames
```

3. Save and quit the file.

▼ To Configure Group Authorization on a NTLM Server

This procedure installs the required tools from the Windows Server Administration Pack that are required for configuring group authorization on an NTLM authentication server. The primary tools are Active Directory Schema MMC Snap-in for adding the attribute “info” to the objectclass “Users”, and the ADSI Edit MMC Snap-in to edit the property “comment” as “group_name=<Group1> [,<Group2,...,GroupN>];

1. Install the tools from the Windows Administration Pack.

2. Select [Start] > [Run] from the Windows desktop.

3. In the Run field type “mmc /a” and click [OK].

A console window appears.

4. Click Console in the console window menu bar and select “Add/Remove Snap-in...”.

The “Add/Remove Snap-in” window appears.

5. Click [Add].

The “Add Standalone Snap-ins” window appears.

6. Select “Active Directory Schema” and click [Add].

7. Select “ADSI Edit” and click [Add].

8. Click [Close].

9. Click [OK] in the “Add/Remove Snap-in...” window.

▼ *To Configure Active Directory Schema*

1. In the console window, double click “Active Directory Schema.”

   The paths “Classes” and “Attributes” appear.
2. Double click “Attributes” and confirm that the “info” attribute is present.
3. Double click “Classes,” locate the class “Users,” and right click to select “Properties.”
4. Select the “Attributes” tab and click [Add].
5. Locate “info” in the attributes list; click [Apply] and then [OK].

▼ *To Configure ADSI Edit*

1. In the console window, double click “ADSI Edit.”
2. In the menu bar, select “Action” > “Connect to...”

   The “Connection” window appears.
3. Use the defaults and Select [OK].

   The path “Domain NC[*domain.com*] appears.
4. Double click “Domain NC[*domain.com*].”

   The expanded path “DC=xxx,DC=*xxx*,DC=com” appears.
5. Double click "DC=xxx,DC=xxx,DC=com.”

   The expanded classes "CN=Builtin, ...“appear.
6. Double click "CN=Users".

   The expanded users list appears.
7. Right click an admin user and select "Properties.”

   The "CN=<username> Properties” window appears.
8. In the Optional, “Select a property to view:” locate [comment].
9. In the “Edit Attribute” field, enter [group_name=admin] and click [OK].
10. Close or save the remaining windows.

Administering Security Certificates for HTTPS and SSH on the OnSite

Configuration of security certificates is required to support the security features in the following list:

- HTTPS (secure HTTP based on SSL)

  Because HTTPS requires an SSL certificate to be installed in the web server, the OnSite automatically generates and installs its own self-signed certificate. The OnSite administrator needs to replace the automatically-generated self-signed certificate.

- SSH authentication through exchange of SSH certificates

  OpenSSH software included in the OnSite supports optional authentication of SSH connections through exchange of X.509 certificates. The OnSite administrator needs to configure support for exchange of X.509 certificates requires configuration

The following table lists the procedures included in this document for administering security certificates. See also publicly available OpenSSL and OpenSSH documentation for additional details.

Table 8-3: Tasks for Administering Security Certificates

Task	Where Documented
Replace the automatically-generated certificate in the Web server with a new certificate generated with your organization's identification.	"Configuring Security Certificates" on page 521 **Note:** The replacement for the automatically-generated certificate is usually used as a placeholder while an official CA-signed certificate is being obtained.

Table 8-3: Tasks for Administering Security Certificates (Continued)

Task	Where Documented
Request, install, and configure a certificate from a CA (certificate authority) OR Create your own local CA and generate a local (less secure but more practical in some environments) **Note:** How to create your own CA is outside of the scope of this document	"Enabling SSH to Use X.509 Certificates" on page 528 **Note:** Installing and configuring a CA-signed certificate is required both for HTTPS and for the optional use of SSL authentication based on the exchange of certificates.
Configure SSH to accept X.509 certificates from clients	"Enabling SSH to Use X.509 Certificates" on page 528

Configuring Security Certificates

OnSite generates its own self-signed SSL certificate for HTTPS. It is highly recommended that you regenerate the local OnSite-generated certificate with identifying data specific to your site, and that you at the same time initiate the process of applying for an official certificate from a certificate authority, such as VeriSign. Use of certificates from known CAs is recommended because many browsers only accept signed certificates from known CAs.

The `openssl.cnf` file must exist for configuring security certificates. By default, `openssl` looks for the file in `/usr/local/ssl`, as shown in the following error message:

```
Unable to load config info from /usr/local/ssl/openssl.cnf.
```

OnSite administrators cannot write into the `/usr` directory, so we recommend putting the file into the `/etc` directory. The file can be downloaded from the Internet or copied from Figure 8-1. The file must be modified to suit your configuration.

```
##################################################################
# openssl example configuration file.
# Mostly used for generation of certificate requests.
##################################################################
[ ca ]
default_ca        = exampleca             # The default ca section

[ exampleca ]

dir               = .                     # Where everything is kept
certificate       = $dir/cacert.pem       # The CA certificate
database          = $dir/index.txt        # database index file.
new_certs_dir     = $dir/certs            # default place for new certs.
private_key       = $dir/private/cakey.pem# The private key
serial            = $dir/serial           # The current serial number
default_crl_days  = 30                    # how long before next CRL
default_days      = 365                   # how long to certify for
default_md        = md5                   # which md to use.
policy            = exampleca_policy
x509_extensions   = certificate_extensions# The extensions to add to the cert

[ exampleca_policy ]
commonName             = supplied
stateOrProvinceName    = supplied
countryName            = supplied
organizationName       = supplied
organizationalUnitName = optional

[ certificate_extensions ]
basicConstraints                        = CA:false

[ req ]
default_bits        = 2048
```

```
default_keyfile      = ./private/cakey.pem
default_md           = md5
prompt               = no
distinguished_name   = root_ca_distinguished_name
x509_extensions      = root_ca_extensions # Extensions to add to the self
                                          # signed cert

[ root_ca_distinguished_name ]
commonName                               = Example CA
stateOrProvinceName                      = mystate
countryName                              = US
emailAddress                             = myname
organizationName                         = Cyclades

[ root_ca_extensions ]
basicConstraints                        = CA:TRUE
################################################################################
```

Figure 8-1: `/etc/openssl.cnf`

The following table shows the tasks for obtaining a signed certificate and where the tasks are documented.

Table 8-4: Tasks for Obtaining an SSL Signed Certificate from a CA

Task	Where Documented
Regenerating the local self-signed certificate so it contains information specific to your organization. (This should usually be done only as a temporary measure while awaiting a signed certificate from a CA.)	"To Configure an SSL Certificate With Your Organization's Data" on page 524
Obtaining a signed certificate from a CA in either of the two following ways: • By setting up a local CA and generating your own certificate • By requesting a certificate from an official CA	"To Obtain an Signed Certificate From a Certificate Authority" on page 526

▼ *To Configure an SSL Certificate With Your Organization's Data*

This procedure generates a new self-signed certificate, replacing the default Cyclades information with information specific to your organization.

Note: Like the default automatically-generated certificate, the certificate generated by this procedure is not CA-generated. It is recommended that you use the resulting self-signed certificate temporarily while waiting for a certificate signing request to be fulfilled by an official CA (as described in "To Obtain an Signed Certificate From a Certificate Authority" on page 526).

---

1. Log into the OnSite console as root.
2. Open the `/etc/req_key` file for editing.

```
[root@onsite /]# vi /etc/req_key
```

3. Replace the default Cyclades data with your organization-specific data.

```
[ req ]
default_bits            = 1024
distinguished_name      = cyclades
prompt                  = no
x509_extensions         = x509v3

[ cyclades ]
C               = US
ST              = CA
L               = Fremont
O               = Cyclades Corporation
OU              = R&D
CN              = www.cyclades.com
emailAddress    = support@cyclades.com

[ x509v3 ]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  =
keyid:always,issuer:always
basicConstraints        = CA:true
nsComment               = "This is just a TEST
certificate. Don't use it for real secure
conections. Create your own certificate instead."
nsCertType              = server, sslCA
```

4. Save and quit the file.

5. Remove the files identified by the wildcard pathname `/etc/CA/*.pem`.

```
[root@onsite /]# rm /etc/CA/*.pem
```

6. Execute the following script.

```
[root@onsite /]# /bin/firstkssl.sh
```

7. Reboot the OnSite or restart the Web Manager.

▼ *To Obtain an Signed Certificate From a Certificate Authority*

Before performing this procedure, generate a private key Also see `http://pki-page.org` for a list of official CAs, if needed.

Make sure that the /etc/openssl.cnf file exists and has been configured properly. You can do one of the following:

- Download the file from the Internet.
- Copy the contents of the file in Figure 8-1.

Note: How to generate the private key is outside the scope of this document. See OpenSSL documentation available on the Internet for more information.

---

1. Log into the OnSite console as root.
2. Use `openssl` with the `req` parameter to create a CSR (certificate signing request).

   Use the command line shown in the following screen example, replacing ***private_key*.pem** with the name of the file that contains the private key.

Note: The command line in the screen example is broken into two lines because of space limitations. You can either enter the whole command on one line or include a backslash (\) as shown to tell the shell that the command continues on the following line.

```
[root@OnSite /]# openssl req -new -nodes -key \
private_key.pem -out cert.csr -config /etc/openssl.cnf
```

The /etc/openssl.cnf must be in /etc directory. The `openssl` utility prompts for the required information shown in the following table. Any other requested information is not required.

Prompt	What You Enter
Country Name (2 letter code) [AU]: Refer to the ISO-3166 two-letter country code list if you do not know your country code.	The country code consisting of two letters.

Prompt	What You Enter
State or Province Name (full name) [Some Country]:	The full name (not the postal abbreviation) of your country
Locality Name (e.g., city) [Some-City or County]:	The name of your city.
Organization Name (e.g., company) [Internet Widgits Ltd]:	The organization for which you want to obtain the certificate
Organizational Unit Name (e.g., section) [Owner]:	The department or section, such as Research and Development.
Common Name (the fully qualified domain name) []:	The fully qualified domain name where the certificate is to be installed
Email Address []:	Contact email address for the applicant.

Note: The generated request includes the public key.

3. Submit the CSR request to the certificate authority (CA).

▼ *To Enable HTTPS By Installing the X.509 Certificate and the Server Key Where the Web Server Can Find It*

This procedure requires a previously-generated private key and a signed certificate from a CA copied to the OnSite.The example shows the files copied into the OnSite's `/root` directory. See "To Obtain an Signed Certificate From a Certificate Authority" on page 526, if needed. This procedure copies the private key and the certificate to a directory where the `AcsWeb` server has been configured to find it.

1. Log into the OnSite console as root.
2. Copy the OnSite's private key and CA-signed certificate into `/etc/CA/server.pem`.

The following screen example uses `cert.crt` as the name of the certificate file and `private_key.pem` as the name of the private key file.

```
[root@OnSite /root]# cat cert.crt private_key.pem > \
/etc/CA/server.pem
```

3. Copy the CA-signed certificate again, this time into the file named `/etc/CA/server.crt`.

   The following screen example uses `cert.crt` as the name of the certificate file. Substitute the correct name for the certificate file.

```
[root@OnSite /root]# cat cert.crt > /etc/CA/server.pem
```

4. Make sure the files where you store the server key and certificate are listed in`/etc/config_files`.

Note: By default `/etc/CA/server.pem` and `/etc/CSA/cert.pem` are listed in`/etc/config_files`.

---

5. Restart the web server to put the certificate into effect.

```
[root@OnSite /root]# daemon.sh restart WEB
```

Enabling SSH to Use X.509 Certificates

The OpenSSH software included with the OnSite has support for X.509 certificates. This section provides the following:

- The prerequisites for enabling and using X.509 certificates for SSH authentication
- The tasks

Prerequisites for Enabling and Using X.509 Certificates for SSH Authentication

To enable the exchange of certificates with a client, the administrator needs to make sure that the prerequisites listed below are complete:

- The client must have installed and enabled an OpenSSH client with the X.509 patch (which is available at http://www.roumenpterov.info/openssh).
- The client must have an SSL certificate issued by a CA and a hostkey.
- For each client connected to a serial port, the serial ports are configured for “socket_ssh” protocol and assigned the IP address of the connected device.
- The OnSite must have a private key and an SSL certificate issued by a CA.

The OnSite administrator must obtain the client information from the client’s certificate and host key, and add the user identification to the authorized keys file as described in the following procedure.

▼ *To Enable Authentication of SSH Sessions Through Exchange of X.509 Certificates*

This procedure requires the following prerequisites to be done:

- The client must have installed and enabled an OpenSSH client with the X.509 patch (which is available at http://www.roumenpterov.info/openssh).
- For each client connected to a serial port, the serial ports must be configured for “socket_ssh” protocol and assigned the IP address of the connected device.

This procedure assumes that `/etc/ssh/authorized_keys` is the filename defined in the `AuthorizedKeysFile` definition in the `sshd_config` file.

Do this procedure for each client with which the OnSite needs to exchange security certificates.

1. On the client, an administrator must extract the client information from the client’s signed certificate and make the information available to the administrator who is configuring the client on the OnSite.

The following screen example shows the command used to obtain the client information and the resulting output from a signed certificate that was generated from a local CA at Cyclades.

```
# openssl x509 -noout -subject -in \
/etc/ssh/ca/ca-bundle.crt
subject= /C=US/ST=CA/L=Fremont/O=Cyclades Corporation/OU=R&D/
CN=www.cyclades.com
```

2. On the OnSite, the administrator must make the following change to the output of the Step 1.
   a. Replace the string "`subject=`" with "`x509v3-sign-rsa disTinguishednamE:`".
   b. Append the edited output to the `/etc/ssh/authorized_keys` file.

   The following screen example shows the tail of the `/etc/ssh/authorized_keys` file after the edited output from Step 1 is appended.

```
x509v3-sign-rsa disTinguishednamE: /C=US/ST=CA/L=Fremont/
O=Cyclades Corporation/OU=R&D/CN=www.cyclades.com
```

3. On the OnSite, the administrator must do the following:
   a. Open the `/etc/ssh/sshd_config` file for editing.

b. Uncomment the lines shown in the following screen example and make the appropriate changes.

```
AllowedCertPurpose sslclient
CACertificateFile /etc/ssh/ca/ca-bundle.crt
HostKey /etc/ssh/ssh_host_key
ChallengeResponseAuthentication no <--
HostbasedAuthentication no
StrictModes no <--
PasswordAuthentication no <--
PubkeyAuthentication yes
RhostsRSAAuthentication no
RSAAuthentication no
UsePrivilegeSeparation yes
```

c. Save and quit the file.

d. Restart SSH.

```
[root@OnSite /root]# daemon.sh restart WEB
```

4. On the client, the administrator must do the following:

a. Open the `/etc/ssh/ssh_config` file for editing.

b. Uncomment t[he lines shown in the following screen example and make the specified changes.

```
AllowedCertPurpose sslserver
Host *
Protocol 2  <--
CACertificate File /etc/ssh/ca/ca-bundle.crt
```

c. Save and quit the file.

d. Restart SSH.

```
[root@OnSite /root]# daemon.sh restart WEB
```

Note: All the file and pathnames edited in this procedure are listed in the `/etc/config_files` file for restoration after upgrade.

Using the CLI Utility

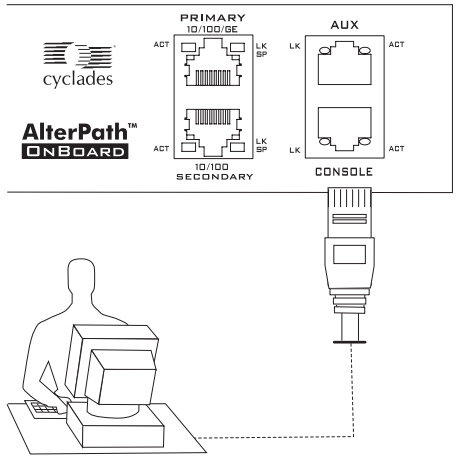
This section describes the `CLI` utility that is available for administrators to use on the OnSite's command line.

Accessing the CLI

The OnSite admin and root users can use the `CLI` command on the command line. Users can access the OnSite command line in any of the following three ways.

- By local logins through the console port

  Local OnSite root users can access the command line by logging in through the console port using a terminal or computer running a terminal emulation program, as illustrated in the following figure.



- By remote logins through SSH, an IPSec VPN tunnel, dial-ins through PPP or a terminal emulation program.
- By accessing the “OnSite console after logging into the Web Manager. After logging into the Web Manager as an administrative user, remote users can access the command line by clicking the “OnSite” menu option.

CLI Utility Features

An administrator (`root` or `admin`) can configure the OnSite using the `CLI` utility. Only one administrator (`root` or `admin`) can run the `CLI` utility at a time. If an administrator is logged into the Web Manager, the `CLI` utility displays a prompt asking if you want to cancel the other administrator’s session.

Administrators often prefer using the `CLI` over the Web Manager because they can run frequently-performed `CLI` configuration commands from shell scripts or from text files that can be executed in batch mode.

The `CLI` utility provides a set of commands that act on parameters that are nested in a format called the CLI parameter tree. Some parameters require arguments when the parameters are entered with some commands. This section describes the `CLI` command and how to navigate the `CLI` parameter tree, but it does not describe all the parameters and values.

The following screen example shows `CLI` entered like any other command on the Linux command line on the OnSite.

```
[root@OnSite root]# CLI

       - Thanks for using the CLI -

This interface allows you to easily modify configurations to
customize and define the functionality of your unit.

Some basic and useful keys are:
 up/down arrow - navigates up/down in the command history
 tab (once/twice) - shows the next possible option(s)

Other hints:
 Put quotes around strings that contain spaces.

Please refer to the Reference Guide for other special keys
and additional information on how to use this interface.

Press TAB to see the list of available options.

cli>
```

Figure 8-2: Invoking the OnSite CLI on the Command Line

As shown in the previous example, usage information appears before the `cli>` prompt appears.

As shown in the previous screen example, the Cyclades `CLI` can be entered at the root prompt. `CLI` can also be entered at the admin prompt that appears when an admin user connects to the OnSite from the Web Manager under Access> Connect to Server. In both cases, `CLI` is being run in interactive mode. See the following sections for definitions of the interactive mode and other execution modes.

Quote strings with spaces using single or double quotes, as shown here: "'string1 string2"'.

Execution Modes

The `CLI` utility has the following three execution modes:

- Command line

  Command line mode refers to when the `CLI` utility is invoked on the Linux command line with options, commands, and parameters and values. See “Command Line Mode” on page 535.
- Batch

  Batch mode refers to when the `CLI` utility is invoked with the `-f` *file* option, or it is invoked from a script, and the commands are executed from the specified file or script. See “Batch Mode” on page 536.
- Interactive

  When invoked without commands, `CLI` enters *interactive mode*; see Interactive Mode.” See “Interactive Mode” on page 536.

Command Line Mode

In command line mode, when the `CLI` utility is invoked on the Linux command line with options, commands, parameters, the utility performs the specified commands, displays any values requested by any command, and returns the Linux shell prompt. To commit the changes made in command line mode, make sure to enter the `CLI` command again followed by `config savetoflash`. See “Saving CLI Changes” on page 540 for more details.

The following screen example shows entering the CLI command with the -s option on the command line in command mode. When the command completes, the shell prompt returns.

```
[admin@OnSite /]# CLI -s config security adduser username \
username
Checking the configuration file list...
Compressing configuration files into /tmp/
saving_config.tar.gz ... done.
Saving configuration files to flash ... done
[admin@OnSite /]#
```

Interactive Mode

Interactive mode is entered by invoking CLI on the command line without commands or other arguments. The cli> prompt appears, and the administrator performs configuration by entering commands followed by parameters followed by parameter arguments at the cli> prompt. The CLI utility waits for new commands until the user enters the quit command.

The following screen example shows invoking the CLI utility, entering a command with the parameters needed to add a new user, saving the newly added user into the configuration files in interactive mode.

```
[root@OnSite /]# CLI
cli> config security adduser username username
cli> config savetoflash
```

Batch Mode

Batch mode is used when CLI commands are run from a file as described in the following bulleted list:

- CLI commands can be saved in a plain text file and executed in batch mode by invoking the CLI utility with the -f *file* option.
- CLI commands can be used in any kind of shell script:
  - #!/bin/CLI can be invoked at the top of a shell script if the script contains only CLI commands.

- Any type of shell can be used to run `CLI` commands along with other commands.

For a very simple example, you could create a script that calls `/bin/CLI` to run in batch mode to configure a hostname for the OnSite as shown in the following screen example.

```
#!/bin/CLI
config network hostsettings hostname FremontCAOnSite
config savetoflash
:wq
```

To run a `CLI` command from the same script that is running other Linux commands, you could put the command in another type of shell script. The `bash` shell is shown in the following example:.

```
#!/bin/bash
...
/bin/CLI -s config network hostsettings hostname
FremontCAOnSite
...
```

To run multiple `CLI` commands from a script that is also running other Linux commands, you could add the multiple `CLI` commands as shown in the following example:.

```
#!/bin/bash
...
/bin/CLI << EOF
config network hostsettings hostname FremontCAOnSite
config security adduser username testuser
config savetoflash
EOF
```

You could then make the script executable and execute it on the command line, as shown in the following screen example.

```
[root@OnSite root]# chmod 777 scriptname2
[root@OnSite root]# ./scriptname2
```

Alternately, you can put one or more commands in a plain text file without invoking any shell as shown in the following screen example.

```
config security adduser username roseanne
```

After you save and quit the file, you can invoke the `CLI` command with the `-f file` option to execute the command(s) from the *file*, as shown in the following example.

```
[root@OnSite root]# CLI -f file
```

Autocompletion

Autocompletion can be used to find out what commands and parameters are available. Pressing the Tab key twice displays all the commands at the top level, as shown in the following screen example.

```
cli> <Tab> <Tab>
administration    info          return   version
applications      portStatus    shell
config            quit          show
```

Pressing the Tab key once after partially-typing a parameter name automatically completes the parameter name, unless there is more than one parameter name beginning with the typed characters. If more than one parameter name begins with the typed characters, then Tab Tab displays them all.

Example:

```
cli> i<Tab>
info
cli> a<Tab> <Tab>
administration applications
cli> sh<TAB>
shell show
```

Pressing the Tab key after a parameter shows the parameters at the next level down in the parameter tree.

Example:

```
cli> config <Tab>
administration  ipmi           restorefromflash   security
applications    network        runconfig
discardchanges  physicalports  savetoflash
```

Saving CLI Changes

Configuration changes made in any of the CLI modes are only temporarily changed in RAM memory. Changes are not saved into the configuration files unless you run the config, runconfig or config savetoflash configuration commands, which are described in the following table.

Table 8-5: CLI Commands for Saving Configuration Changes

Command	Action
config runconfig	Saves configuration changes in the appropriate configuration files.
config savetoflash	Saves any unsaved configuration changes in the configuration files and creates a zipped backup copy of the files in a backup directory for possible later retrieval.
config discardchanges	Restores the backed up configuration files, overwriting any configuration changes made since the last time the savetoflash option was executed.

See the sections describing the various modes for examples of how to save configuration changes.

Using CLI Hot Keys

The CLI hot keys can be used to perform the following types of actions:

- Move the cursor on the command line
- Move through the list of commands in the command history
- Edit characters on the command line.

The following table shows CLI hot keys that are supported in interactive mode.:

Key	Action
Ctrl a	Move to the start of the current line.
Ctrl e	Move to the end of the line.
Ctrl b	Move back a character (same as the left arrow key).
Ctrl f	Move forward a character (same as the right arrow key).
Esc b	Move back to the start of the current or previous word. Words are composed of letters and digits.
Esc f	Move forward to the end of the next word. Words are composed of letters and digits.
Ctrl l	Clear the screen and redraw the current line, leaving the current line at the top of the screen.
Ctrl n	Move `forward' through the history list, fetching the next command (same as <down arrow key>).
Ctrl p	Move `back' through the history list, fetching the previous command (same as <up arrow key>)
Ctrl d	Delete the character under the cursor (same as <delete key>)
Ctrl h	Same as <Backspace key>
Ctrl k	Kill the text from the cursor to the end of the line.
Ctrl u	Kill backward from the cursor to the beginning of the current line.
Ctrl w	Kill the word behind point.
Esc d	Kill from point to the end of the current word, or if between words, to the end of the next word
Esc Tab	Displays the current value of the parameter keyword entered. You can then edit the value

Viewing the CLI Command History

The CLI command history buffer stores last 500 commands. The history is cumulative, so terminating the CLI session does not clear the buffer. So, for example, a user can invoked the CLI and go back over the commands entered in a previous session.

The following screen example shows how to display the current value for the domain.

```
cli> config network hostsettings
hostsettings> domain <Esc> <Tab>
hostsettings> domain cyclades.com
```

The cursor is inserted at the end of the value, in this case at the end of the domain name cyclades.com. You can then backspace or use other hot keys to edit the domain name and then press Enter when done to make the change.

Using CLI Global Commands

The CLI global commands that can be entered at any level of the CLI are shown in the following table.

Table 8-6: CLI Global Commands

Command	Action
quit	Ends the CLI session.
return	Returns to the next level up.
info	Shows the help info available for the current level. See “Info” on page 542.
show	Displays the configuration parameter(s). Valid only in the config> state. See “Show” on page 544.

When the info or show commands are entered at the prompt for the current level, information or parameters that apply to the current level appears. When these commands are entered along with the name of a command supported at the current level, they display information or parameters that apply to the command mode.

Info

The following screen example illustrates the use of the `info` command. Entering `info administration` at the `cli>` prompt displays the same help as entering `info` at the `administration>` prompt.

```
cli > info administration

   - Administration Mode  -

In this mode, you can save or retrieve the unit's
configurations,

list or kill sessions, and/or upgrade the unit's
firmware.

cli> administration

administration> info

   - Administration Mode  -

In this mode, you can save or retrieve the unit's
configurations,

list or kill sessions, and/or upgrade the unit's
firmware.
```

If the output from the `info` command is greater than the screen capacity, the user can type **`m`** to see more, **`b`** to go back to a previous screen, or **`q`** for quit.

Show

The following screen example shows the use of the show command. After entering `config physicalports 1`, entering `show general` at the `Ports[1}` prompt displays the configuration parameters set for the selected serial port.

```
cli> config physicalports 1
Ports[1]> show general

general:
alias:
protocol: consoletelnet
speed: 9600
flow: none
parity: none
datasize: 8
stopbits: 1
```

CLI Options

The following table shows options that can be entered when invoking the `CLI`.

Table 8-7: `CLI` Options

Option	Description
`q`	Suppresses the output of error messages from the `CLI`.
`t time`	The timeout in minutes. Default =10 minutes.
`T`	Disables idle timeout. Same as "`-t 0`."
`s`	Save changes to flash. Same as `savetoflash`). Batch mode only.
`r`	Activate changes. Same as `runconfig`. Batch mode only.
`f` *`filename`*	Executes the commands in the file *`filename`*.

▼ *To Add a User With CLI*

1. Log into the OnSite console and bring up the `CLI` utility.
2. Add the user by entering the parameters shown in the following screen example.

```
cli> config security adduser username username
```

3. Configure the user's password by entering the parameters shown in the following screen example.

```
cli> config security passwd username username newpassword
password
```

4. Configure the user's shell by entering the parameters shown in the following screen example.

```
cli> config security adduser username username shell shell
```

5. Configure comments (UNIX GECOS information) by entering the parameters shown in the following screen example.

```
cli> config security adduser username username comments
comments
```

6. Save the changes

```
cli> config savetoflash
```

7. Quit.

```
cli> quit
[root@OnSite root]#
```

Configuring Dial-Out

Dial-out through the OnSite is required by certain applications used in computer management that poll devices for status or other information. The OnSite supports dial-out through GPRS (GSM) and 1xRTT (CDMA) wireless PCMCI cards. For PCMCIA card slot 1, the device name is `ttyM1`; for slot 2, the device name is `ttyM2`.

The dial-out application connects the port to a remote TCP socket at the specified IP address through a wireless phone network service and an Internet access service.

Prerequisites for Dial-Out Through the OnSite

The prerequisites for dial-out through the OnSite are shown in the following list:

- A CDMA or GSM/GPRS PCMCIA card must be installed and configured.
- The CDMA or GSM wireless phone service must be available.
- An Internet access service must be available.

Tasks for Configuring Dial-Out

The OnSite administrator needs to do the following tasks on the command line to configure dial-out.

Table 8-8: Tasks for Configuring Dial-out

Task	Where Documented
Edit the `/etc/generic-dial.conf` to enable dial-out for the port.	“Configuring the /etc/generic-dial.conf File” on page 547
Configure the `/etc/ppp/peers/wireless` file or create another peers file in `/etc/ppp/peers`.	“Configuring the /etc/ppp/peers File” on page 552
Configure the `/etc/chatscript/wireless` file or create another chat file in `/etc/chatscript`.	“By default, the /etc/ppp/peers/wireless initiates a dial-in connection by reading the chat script configured in the /etc/chatscripts/wireless file.” on page 554

Table 8-8: Tasks for Configuring Dial-out

Task	Where Documented
Edit `/etc/pcmcia/serial.opts` file as follows: • If the GSM card SIM requires a PIN, specify the PIN • Inactivate mgetty on the port to allow the port to be controlled by the `pppd` application.	"Configuring the /etc/pcmcia/serial.opts File" on page 555
Create a static route on the OnSite to the network where the device resides or to the device itself.	"Configuring Automatic Restart and Starting Dial-Out" on page 555
Configure automatic restart of dial-out after a reboot, and start dial-out.	"Configuring Automatic Restart and Starting Dial-Out" on page 555

Configuring the /etc/generic-dial.conf File

The file `/etc/generic-dial.conf` defines dial-out instances in the format shown in the following example.

```
# begin application-type [instanceID]
#....
#....
# end application-type
```

where instanceID is an optional string to identify a particular instance.

The only supported *application-type* is `dial-out`.

The following table shows the parameters that define a `dial-out` instance.

Parameter	Description
`begin dial-out [instanceID]`	Begins the dial-out instance. Optionally specify a name for the particular instance.
`inPort.name name`	A label for the incoming port to be used in log messages.

Parameter	Description
inPort.device /dev/tty*XX*	The device name for the port to be controlled by the generic_dial protocol. For dial-out through a wireless modem device, either ttyM1 or ttyM2.
inPort.speed *speed*	Connection speed. Default = 9600.
inPort.datasize *number*	The number of data bits. Default = 8.
inPort.parity [none | even | odd]	None, even, or odd.
inPort.stopbits *number*	The number of stop bits. Default = 1.
inPort.flowctrl [none | hw | sw]	Gateway or interface address used for the route.
outPort.name *name*	A label for the outgoing port to be used in log messages.
outPort.pppcall *filename*	Name of file from which the pppd reads options, located at /etc/ppp/peers/*filename*. The default outPort.pppcall filename is wireless, which tells the application to read options from the /etc/ppp/peers/wireless file. If the administrator chooses to create another file in /etc/ppp/peers, the administrator must change the outPort.pppcall definition to specify the new filename.
outPort.remote_ip *IP_address*	The IP address of a device. The dial-out application opens a TCP socket connection to the device at the specified IP address.
outPort.remote_port *port*	Remote TCP port to which the socket connection is made.

Parameter	Description
`outPort.connection [permanent | on_demand]`	One of the following options for maintaining the connection: • `permanent` – always connected. • `on_demand` – connects only when data enters through the serial port.
`outPort.timeout` *`timeout`*	The inactivity time in seconds after which the connection is dropped. Any value other than zero enables the time-out. Default = 0.
`appl.retry` *`interval`*	Specify the time in minutes to wait before reconnecting after a connection failure.Default = 5.
`end dial-out`	Ends the dial-out instance.

The following screen example shows the tail of an `/etc/generic-dial.conf` file with a dial-out instance defined. Because the GSM wireless card is installed in slot1, `inPort.device` is defined as `/dev/ttyM1`. The `outPort.ppppcall` is defined as `wireless` to tell the application to read options from the `/etc/ppp/peers/wireless` file. `outPort.remote_ip` defines the IP address of the computer where the remote socket connection is to be made is `200.246.93.87`. The port

number is defined as `7001`. An `appl.retry` definition is added that changes the number of retries from the default of `5` to `7`.

```
begin dial-out Example

inPort.name             InPort
inPort.device           /dev/ttyM1

outPort.name            OutPort
outPort.pppcall         wireless
outPort.remote_ip       200.246.93.87
outPort.remote_port     7001

appl.retry              7

end dial-out
```

▼ To Configure the /etc/generic-dial.conf File

Perform this procedure as the first step to configure dial-out. It edits the `/etc/generic-dial.conf` file to configure the following:

- The device name for the port
- The peer filename
- The IP address and the port number of the device to which the TCP socket connection is to be made.

See the examples in the file for other options that can be set.

1. Open the `etc/generic-dial.conf` file for editing.

2. Remove the pound signs from the sample dial-out instance.

```
begin dial-out testApp

inPort.name             InPort
inPort.device           /dev/ttyS1

outPort.name            OutPort
outPort.pppcall         wireless
outPort.remote_ip       192.168.160.10
outPort.remote_port     7002
outPort.connection      on_demand

end dial-out
```

3. Change the instance name, `inPort.name`, and `outPort.name` if desired.
4. Make sure the device name defined for `inPort.device` is correct for the port where the modem is installed.

   The device name for PCMCIA modem cards should be `/dev/ttyM1` for slot 1or `/dev/ttyM2` for slot 2.
5. Make sure that the `wireless` filename defined for `outPort.pppcall` is correct.

   The default file in `/etc/ppp/peers` is wireless. If you create another peers file with another name, enter it instead.
6. Define `outPort.remote_ip` with IP address of the device to which the TCP socket connection is to be made.
7. Define `outPort.remote_port` with the port number to which the TCP socket connection is to be made.
8. Save and quit the file.
9. Go to "Configuring the /etc/ppp/peers File."

Configuring the /etc/ppp/peers File

The default file in `/etc/ppp/peers` is called `wireless`. The `wireless` file reads a chat script from the `/etc/chatscripts/wireless` file.

The following figure shows an example `/etc/ppp/peers/wireless` file.

```
[root@OnSite root]# more /etc/ppp/peers/wireless
nodetach
#debug
/dev/ttyM1
57600
crtscts
lock
noauth
#nomagic
user claro
show-password
noipdefault
defaultroute
ipcp-accept-local
ipcp-accept-remote
noproxyarp
novj
novjccomp
lcp-echo-interval 0
connect '/usr/local/sbin/chat -v -t3 -f /etc/chatscripts/wireless'
```

Figure 8-3: Example `/etc/ppp/peers/wireless` File

The example `/etc/ppp/peers/wireless` file shown in Figure 8-3 makes the following definitions:

- Defines `/dev/ttyM1` as the port
- Defines a user named claro: `user claro`.
- Tells `connect` to initiate the connection using `/usr/local/sbin/chat` with the parameters:
  - `-v` executes the script in verbose mode
  - `-t3` sets the timeout to 3 seconds
  - `-f /etc/chatscripts/wireless`, tells the application to read the chat script from the specified file.

If the administrator chooses to create another chat file in `/etc/chatscripts`, the administrator must change the filename specified after the `-f` option to the new filename and specify the new filename in the `outPort.pppcall` definition in the `/etc/generic-dial.conf file`.

▼ To Configure the /etc/ppp/peers/wireless File

This procedure configures the device name for the port, the user name, and other optional values in the peers file in `/etc/ppp/peers` using the default filename `wireless`.

1. Open the `/etc/ppp/peers/wireless` file for editing.
2. Enter the device name for the port.

   The following screen example shows `/dev/ttyM1` entered as the device name for PCMCIA card slot 1.

```
[root@OnSite root]# vi /etc/ppp/peers/wireless
nodetach
#debug
/dev/ttyM1
```

3. Enter the user name after the `user` keyword.

```
user claro
```

4. Make any other edits you desire.
5. Save and quit the file.
6. Go to "By default, the /etc/ppp/peers/wireless initiates a dial-in connection by reading the chat script configured in the /etc/chatscripts/ wireless file.."

Configuring the /etc/chatscripts/wireless File

By default, the `/etc/ppp/peers/wireless` initiates a dial-in connection by reading the chat script configured in the `/etc/chatscripts/wireless` file.

```
ABORT   BUSY
ABORT   VOICE
ABORT   "NO CARRIER"
ABORT   "NO DIALTONE"

""      AT
""      ATZ

####    Telco X
OK     AT+CGDCONT=1,"IP","claro.com.br"
OK     ATD*99#

####    Telco Y
#OK     AT&C0
#OK     ATDT#777

CONNECT ""
```

Figure 8-4: Default `/etc/chatscripts/wireless` File

The example specifies the following AT commands:

- An ATD command to dial the "*99#" number
- An AT+CGDCONT=1,"IP","claro.com.br" to contact a local GPRS broadband service (GSM wireless network) in Brazil.

▼ To Specify the Telephone Carrier in the /etc/chatscripts/wireless File

1. Open the `/etc/chatscripts/wireless` file for editing.
2. Remove the pound signs (#) next to one of the `Telco` definitions .
3. Modify the commands to initiate the contact with your GSM/CDMA wireless service provider and to dial the correct number.
4. Save and quit the file.
5. Go to "Configuring the /etc/pcmcia/serial.opts File."

Configuring the /etc/pcmcia/serial.opts File

Perform the following procedure to do the following:

- Set a PIN, when required by a GSM wireless phone card
- Deactivate `mgetty` on the port to allow the port to be directly controlled by the `pppd` application

▼ To Set a GSM Pin and Deactivate mgetty in the /etc/pcmcia/serial.opts File

1. Open the `/etc/pcmcia/serial.opts` file for editing.
2. If the wireless phone card is a GSM card that requires a PIN, uncomment the following line and replace `1111` with the PIN.

```
INITCHAT="- \d\d\d+++\d\d\datz OK at+cpin=1111 OK"
```

3. Comment out the `INITTAB="/sbin/mgetty"` link, to deactivate `mgetty` on the port.

```
#INITTAB="/sbin/mgetty"
```

4. Save and quit the file.
5. Go to "Configuring Automatic Restart and Starting Dial-Out."

Configuring Automatic Restart and Starting Dial-Out

The administrator should do the following procedure after editing the configuration files in the previous procedures:

- Enable the “automatically established” feature in the `/etc/daemon.d/gendial.sh` file to automatically restart the dial-out function after a reboot.
- Activate dial-out by restarting the GDF daemon.

▼ To Configure Automatic Restart of Dial-Out in the /etc/daemon.d/gendial.sh File

1. Open the `/etc/daemon.d/gendial.sh` file for editing.
2. Set the ENABLE = YES.

```
ENABLE = YES
```

3. Save and quit the file.

▼ To Restart the GDF Daemon to Activate Dial-Out

1. Enter the `daemon.sh restart GDF` command to restart the GDF daemon.

```
[root@OnSite root]# daemon.sh restart GDF
```

A message similar to the following displays, confirming that the GDF daemon restarted.

```
[root@OnSite root]# Sep 23 18:06:10 src_dev_log@OnSite
showlogmsg: /bin/daemon.sh: CONFIG: Network daemon [generic-
dial] started
```

The default route is not replaced in the static router table. The following message displays.

```
[root@OnSite root]# Sep 23 18:06:17 src_dev_log@CAS
pppd[1028]: not replacing existing default route to eth0
[172.20.0.1]
```

2. Go to "To Configure a Static Route for Dial-Out."

▼ To Configure a Static Route for Dial-Out

1. Open the `/etc/network/st_routes` file for editing.
2. Add the desired static route(s) to the file.

3. Save and quit the file.
4. Check the route(s) by issuing the following command.

```
[root@OnSite root]# route -n
```

Configuring Dial-Out Through Modems Accessed as Serial Devices

Although only wireless PCMCIA cards are tested and supported, the OnSite can be configured to dial out through any modem that can be connected to or viewed as a serial device, including any of the following:

- An external modem connected to one of the following:
  - Either of the OnSite's AUX ports `ttyA1` or `ttyA2`
  - The OnSite's console port
  - Any of the OnSite's serial ports `ttyS1` through `ttyS`
- The internal V.90 modem in the OnSite at `ttyA3`
- A non-wireless modem PCMCIA card at `ttyM1` or `ttym2`

The OnSite administrator needs to do the following

- Edit `/etc/portslave/pslave.conf` to configure the port with the "generic-dial" option, which prevents `portslave` from being started on the port and starts the generic application that manages dial-out instead.
- Do all the tasks in Table 8-8, "Tasks for Configuring Dial-out," on page 546.

▼ To Configure Serial Ports for Dial-Out

Perform this procedure to enable dial-out through a modem connected to any of the ports described under "Configuring Dial-Out Through Modems Accessed as Serial Devices" on page 557. See "Port Numbers and Aliases" on page 47 for port numbers for ports on the OnSite.

1. Open the `/etc/portslave/pslave.conf` file for editing.
2. Define `generic_dial` as the protocol for the port to which the modem is connected.

The following screen example shows the format.

```
s<N>.protocol  generic_dial
```

where <*N*> is the serial port number.

3. Perform the configuration steps, specifying the correct port number, as described in Table 8-8, “Tasks for Configuring Dial-out,” on page 546.

Chapter 9
Troubleshooting

This chapter provides information related to troubleshooting the OnSite.

The following table lists the sections in this chapter.

This chapter also provides the troubleshooting procedures shown in the following sections.

Connection Methods for Troubleshooting

This section summarizes how to connect to the OnSite for troubleshooting in the event of an IP network failure.

Remote OnSite administrators can connect to the OnSite using any of the following methods:

- By using `telnet` or `ssh` and supplying the OnSite's IP address
- By bringing up the Web Manager over PPP after establishing a dial-in or callback connection to any of the following modem types:
  - The internal modem
  - An external modem optionally connected to the OnSite
  - A modem on a PCMCIA modem card (including GSM and ISDN) optionally installed in the OnSite

Local OnSite administrators can connect to the OnSite using any of the following methods:

- Logging into the OSD through a locally connected KVM management (Local user) station
- Logging into the Linux command line of the OnSite through either of the following:
  - A terminal or computer connected to the OnSite's console port
  - A dumb terminal connected to a serial port and configured with the Local Terminal protocol

All of these connection methods must be previously configured as described elsewhere. For example, to use a modem on a PCMCIA card, the PCMCIA modem card must be configured as described in "To Begin Configuring a PCMCIA Card [Expert]" on page 306.

The following table shows the tasks for configuring the troubleshooting connection methods.

Table 9-1: Tasks for Configuring Troubleshooting Connection Methods [OSD]

Connection Method	Where Configuration is Documented
Internal modem	• "Configuration>Serial/AUX>Aux/Modem Port" on page 257 • "To Configure the Internal Modem [Expert]" on page 267
External modem	• "To Configure an AUX Port for PPP [Expert]" on page 266
Local User station	• "To Configure Local User Sessions [Expert]" on page 221

Recovering from root Authentication Failure

Use the following procedure if an attempt to login to the console as root brings up the following message.

```
login[212]: FAILED LOGIN
1 FROM FOR root, User not known to the underlying
authentication module
Login incorrect
```

▼ *To Recover from root Authentication Failure*

1. Boot the OnSite in the single user mode.

   See "To Boot in Single User Mode from U-Boot Monitor Mode" on page 571. The root single user prompt appears as shown in the following screen example.

```
[root@(none) /]#
```

2. Open the `/etc/nsswitch.conf` file for editing.

```
[root@(none) /]# vi /etc/nsswitch.conf
```

3. Search for the uncommented entries for the `passwd`, `shadow` and `group` databases [whose lines do not start with the pound (#) sign].

For example, in the portion of the `nsswitch.conf` file in the following screen example, no pound (#) signs appear before the entries for the `passwd`, `shadow`, and `group` databases under `NISLocal`.

```
# NISLocal
passwd:     nis files
shadow:     nis files
group:      nis files
```

4. Change the search order to `files` only for the uncommented `passwd`, `shadow`, and `group` databases.

```
# NISLocal
passwd:     files
shadow:     files
group:      files
```

5. Save and quit the file.
6. Open the `/etc/portslave/pslave.conf` file for editing.

```
[root@(none) /]# vi /etc/portslave/pslave.conf
```

7. Change the `conf.authtype` parameter back to `local`.

```
# by default, authentication to the box is local
conf.authtype   local
```

8. Save and quit the file.
9. Restart the OnSite to return to multiuser mode.

```
[root@(none) /]# reboot
```

You should be able to log in as root.

10. Reconfigure authentication as desired.

Restarting the Web Manager

If the Web Manager stops responding the web server may be either inactive or stopped. Perform this procedure to stop and restart it.

▼ *To Restart the Web Manager*

1. Enter the `ps` command with the `-ef` option and look for a line with `/bin/AcsWeb`, as shown in the following screen example.

```
[root@ONS root]# ps -fe | grep Acs
13495 ttyS0 root 8540 S /bin/AcsWeb
```

- If a line like the one shown in the screen example appears, go to Step 2.
- If `/bin/AcsWeb` is not running, go to Step 2.

2. Enter the `daemon.sh` command with the `stop WEB` option as shown in the following screen example.

```
[root@ONS root]# daemon.sh stop WEB
```

3. Enter the `daemon.sh` command with the `WEB` option as shown in the following screen example.

```
[root@ONS root]# daemon.sh WEB
```

4. Enter the `ps` command with the `-ef` option again as in Step 1 to verify the Web server has been activated.

Replacing a Boot Image for Troubleshooting

Information in “Boot File Location Information” on page 566 in Appendix A, “Advanced Boot and Backup Configuration Information” gives an OnSite administrator who has the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

Network boots are recommended for troubleshooting. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the removable flash memory becomes corrupted, you could download the software to a tftpboot server, and then save it to the removable flash after testing, using the `create_cf` command.

Using the create_cf Command When Troubleshooting

You can use the `create_cf` command when troubleshooting problems with the boot image, as described under “To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode” on page 572. Use it carefully as described in “Options for the create_cf Command” on page 577.

Using the restoreconf Command When Troubleshooting

As described in other sections of this chapter, you may need to use the `restoreconf` command while troubleshooting. All the `restoreconf` subcommands are described under “Options for the restoreconf Command” on page 580

A
Advanced Boot and Backup Configuration Information

This appendix provides information related to configuring boot file locations and managing configuration file changes on the AlterPath OnSite.

The following table lists the sections in this appendix.

This appendix also provides the troubleshooting procedures shown in the following sections.

Boot File Location Information

The information in this section is needed to understand how to configure booting through the Web Manager, as described in "Configuration>System>Boot Configuration" on page 351. This information is also needed for troubleshooting, to give an administrator who has the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

The OnSite uses a U-Boot boot loader that resides in soldered flash memory and that automatically runs at boot time. U-Boot boots the OnSite from an image whose location is configurable. The image can reside either in removable flash memory on the OnSite or on a boot server on the network. Each image on the removable flash has three separate file systems mounted on three Linux partitions. The first partition for each image contains the kernel, the second partition contains the root filesystem mounted read only, and the third partition contains the configuration files mounted read-write.

For more about U-Boot in general, go to: http://sourceforge.net/projects/u-boot.

The OnSite boots from alternate images as described below.

- The OnSite initially boots from a software image referred to as "image1," which is stored in three partitions on the removable flash (`hda1`, `hda5`, and `hda7`).
- The first time you download and install a new software version from Cyclades, the new image is stored as "image 2" in another set of three identical partitions on the removable flash (`hda2`, `hda6`, and `hda8`), and the configuration is changed to boot the OnSite from "image2."
- The second time you download a new software version, the latest image is stored as "image1" in the first set of three partitions, and the OnSite configuration is changed to boot from "image1."
- Subsequent downloads are stored following the same pattern, alternating "image1" with "image2."

Each image has three separate filesystems mounted on three Linux partitions. Refer to the following text and figure explaining partition numbers if needed for understanding some of the instructions in the rest of this chapter. As illustrated in the following figure, the first partition for each image contains the Linux kernel, the second partition contains the root-mounted filesystem

(which is mounted read only), and the third partition (which is mounted read write) contains the configuration files.

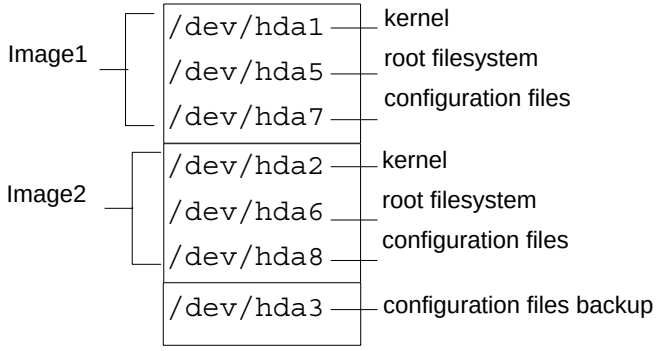


Figure A-1: Boot Partitions

The previous figure also shows a configuration backup partition (`/dev/hda3` in removable flash). This partition is mounted as `/mnt/hda3`. The `/mnt/hda3/backup` directory contains compressed copies of backed up configuration files, as shown in the following screen example.

```
[root@ONS /]# cd /mnt/hda3/backup
[root@ONS /]# ls
configuration_files.gz
```

Downloading a New Software Version

You can download a new software version in either of the following ways:

- Use the Web Manager → Firmware Upgrade screen to download the image from an FTP server

  When the image is downloaded by FTP, a script (`saveimage`) automatically extracts the filesystem from the image, mounts it, and copies the files to the removable flash. Since the current image is being run from one of the three-partitions sets, the downloaded image is stored in the other set of three partitions. The environment variable

`currentimage` is changed so that the system boots from the new image.

- Do a network boot from the image and then save it onto the removable flash

  The U-Boot monitor command `net_boot` boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if no removable flash card is inserted.

  From the command line, you can then run the `create_cf` script with the `--doformat` option to automatically save the image from RAMDISK into the removable flash. The script erases everything in the flash, partitions the flash, if necessary, formats the partitions, and copies the files currently in the RAMDISK into the corresponding image partitions. If the flash is already partitioned, you can choose where the image is saved using the option `--imageN`.

Changing the Boot Image

If, for any reason, you want to change to another image from the current one, if you have access to the Web Manager, you can use the Config → Boot Configuration screen to select the other image, and then use the "Restart" button on the Mgmt → Restart screen to boot the OnSite from the new location.

You have two other options if you cannot access the Web Manager:

- Use the `CLI` utility

  See "To Boot from an Alternate Image Using CLI" on page 568.

- Boot in U-Boot monitor mode and use the available boot commands

  See "To Boot in U-Boot Monitor Mode" on page 570.

▼ *To Boot from an Alternate Image Using CLI*

1. Connect to the OnSite from a terminal connected to the console port or create a `telnet` or `ssh` connection, and log in as root.
2. Enter the `CLI` command.

```
# CLI
```

The `cli>` prompt appears.

```
cli>
```

3. Enter `config administration bootconfig`.

```
cli> config administration bootconfig
```

The `bootconfig>` prompt appears.

```
bootconfig>
```

4. Enter the `bootunit` keyword followed by the Tab key to see the list of possible boot values

```
bootconfig>bootunit <Tab>
image1:zvmppcons.v100
image2:zvmppcons.v101
network
bootconfig>
```

5. Enter the name of the boot image you want to use.

   If you type a unique string of characters from the image name and then press the Tab key, it autocompletes the name for you. For example, typing **`bootunit image2`** and pressing Tab causes the full file name `image2:zvmppcons.v101` to be filled in, as shown in the following screen example.

```
bootconfig>bootunit image2:zvmppcons.v101
```

The `currentimage` environment variable is changed to boot from the specified image.

Changing the Boot Image in U-Boot Monitor Mode

You can access U-Boot monitor mode in one of the following two ways:

- During boot, when the “Hit any key to stop autoboot” prompt appears, pressing any key before the timer expires brings the OnSite to U-Boot monitor mode.
- If boot fails, the OnSite automatically enters U-Boot monitor mode.

The U-Boot `hw_boot` command boots from either the first or second image according to the value of the `currentimage` environment variable. You can use the following procedures to change which image is used for booting.

▼ To Boot in U-Boot Monitor Mode

1. Open a terminal connection to the console port, and log in as root.
2. Enter the `reboot` command.

```
# reboot
```

   During boot, when the “Hit any key to stop autoboot” prompt appears, press any key before the time elapses to stop the boot.

   The U-Boot monitor prompt appears:

```
=>
```

3. Enter `help` to see a list of supported commands.

```
=> help
```

▼ To Boot from an Alternate Image in U-Boot Monitor Mode

1. Go to U-Boot monitor mode.

   See "To Boot in U-Boot Monitor Mode" if needed.

2. Set the current image environment variable to the number of the image you want to boot.

```
=> setenv currentimage N
```

   For example, to boot from image2 enter the number 2, as shown in the following screen example.

```
=> setenv currentimage 2
```

3. Enter the boot command.

```
=> hw_boot
```

▼ To Boot in Single User Mode from U-Boot Monitor Mode

1. See “To Boot in U-Boot Monitor Mode” on page 570 if needed.

2. Boot by entering `hw_boot` followed by `single`, as shown in the following screen example.

```
=> hw_boot single
```

3. The single-user # prompt appears, as shown in the following screen example.

```
[root@(none) /]#
```

Network Boot Options and Caveats

When a network boot is performed with the U-boot `net_boot` command, the OnSite boots from the specified image on the specified TFTP server. The image uses the RAMDISK as the root file system. Network boots are useful for troubleshooting because the net-booted image can run even if the OnSite's flash memory is not usable.

Network boots are recommended only for troubleshooting and must not be used for normal operation of the OnSite. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the resident flash memory becomes corrupted, you could download the software from a tftpboot server, and then save it to the removable flash after testing, using the `create_cf` command with the appropriate options (see "Options for the create_cf Command" on page 577).

When a network boot is performed, the system uses one of the two following sources of configuration data:

- If the `net_boot` command is entered with the `configsource=factory_default` option, the factory_default configuration files are restored.
- Otherwise, the backed up configuration files from the `/dev/hda3` backup partition are copied to the RAMDISK and used.

Any configuration changes made after the last backup copy was made are lost unless the configuration files were backed up before the network boot and then restored afterwards (see "How Configuration Files Changes Are Managed" on page 574).

▼ *To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode*

1. Log in as root in U-boot monitor mode.

If needed, see, '"To Boot in U-Boot Monitor Mode" on page 570.

2. Set the “bootfile,” “serverip,” and “ipaddr” environment variables using the boot filename, the TFTP boot server’s IP address, and the IP address of the OnSite to use for network booting.

```
=> setenv ipaddr OnSite’s_IP_address
=> setenv serverip boot_server’s_IP_address
=> setenv bootfile boot_file’s_name
```

   The format of the boot filename is: `zmppcons.v`*`version_number`*, for example: `zmppcons.v110`. See the following screen example.

```
=>setenv ipaddr 193.168.45.29
=> setenv serverip 193.168.46.127
=> setenv bootfile zvmppconb.v110
```

3. Check that the environment variables are set properly with the `printenv` command.

```
=> printenv
bootfile=zvmppconb.v110
ipaddr=192.168.45.29
serverip=192.168.46.127
```

4. Enter the `net_boot` command.

```
=> net_boot
```

5. Log in as root after boot completes.
6. Run the `create_cf` command with the `--doformat` option.

```
[root@OnSite root]# create_cf --doformat --factory_default
```

Note: Be aware that the `--doformat` option erases the flash memory and installs the boot image into the image1 area. See “Options for the create_cf Command” on page 577 for other options.

7. The following text appears when the operation completes.

```
Creation of image N completed.
...
```

8. Configure the OnSite to boot from flash.

See “To Boot from an Alternate Image in U-Boot Monitor Mode” on page 571, if needed.

9. Enter the `reboot` command.

```
# reboot
```

How Configuration Files Changes Are Managed

Changes to configuration files can be made without backing up the configuration files by performing the actions shown in the following table.

Table A-1: Options for Saving Configuration File Changes

Environment	Action
Web Manager	Click the “try changes” button.
OSD	Select the “Save” button on any configuration screen.

Changes made to the configuration files persist after a reboot. If you upgrade software, any changes to configuration files are brought forward after the upgrade. (This allows you to upgrade software on the OnSite without losing all your user configurations.)

Changes to configuration files can be both made and backed up in different environments on the OnSite by performing the actions shown in the following table.

Table A-2: Options for Saving and Backing Up Configuration File Changes

Environment	Action
Web Manager	Click the “apply changes” button.
OSD	Go to Save/Load Config. and select the “Save Configuration” option.
OnSite Linux command line	Enter the `saveconf` command
OnSite CLI utility	Enter the `CLI config savetoflash` command

Saving a backup copy of the configuration files allows an administrator to restore the backed up configuration files even after a reboot or after a software upgrade to overwrite all changes made to the configuration files since the last save.

The system software updates the affected configuration files and creates a compressed copy of the configuration files in `/mnt/hda3/backup/configuration_files.gz` on the resident flash memory. If a compressed configuration file already exists in the backup directory, it is overwritten. The file and the `backup` directory are shown in the following screen example.

```
[[root@ONS /]# ls /mnt/hda3/backup
configuration_files.gz
```

Backed-up changes to configuration files can be restored by performing the actions shown in the following table.

Table A-3: Options for Saving Configuration File Changes

Environment	Action
Web Manager	Click the “cancel changes” button.
OSD	Go to Save/Load Config. and select the “Load Configuration” option.

Table A-3: Options for Saving Configuration File Changes

Environment	Action
OnSite Linux command line	Enter the `restoreconf` command
OnSite CLI utility	Enter the `CLI config restorefromflash` command

How Factory Defaults Are Saved

A compressed copy of the factory default configuration files is stored in the `factory_default_files.gz` compressed file for possible restoration in the `/mnt/hdCnf/backup` directory. The following screen example shows the file.

```
[root@ONS /]# ls /mnt/hdCnf/backup
factory_default_files.gz
```

Restoring Configuration Files

The following table provides links to where the procedures for restoring configuration files are described.

▼ To Restore the OnSite Configuration Files to the Last Saved Version

This procedure assumes that you or a previous administrator has previously run the `saveconf` command, or clicked the "Save" button on the Web Manager Mgmt → Backup/restore screen after making changes to the configuration. This procedure restores the configuration files to the state they were in when they were last backed up.

1. If you are logged into the Web Manager as an administrative user, click the "Load" button on the Web Manager Mgmt > Backup/restore screen.

2. If you are logged into the OnSite console as root through the console port, via `telnet` or `ssh`, enter the `restoreconf` command.

```
[root@ONS /]# restoreconf
```

▼ *To Restore the OnSite Configuration Files to the Factory Defaults*

Use one of the commands shown below while logged in as root through the console, via `telnet`, or via any `ssh` session to restore the configuration files to the state they were in when the OnSite shipped.

- Enter the `restoreconf` command with the `factory_default` option.

```
[root@ONS /]# restoreconf factory_default
```

- Enter the `create_cf` command with the `--factory_default` option.

```
[root@ONS /]# create_cf --factory_default
```

Options for the create_cf Command

Use the `create_cf` command carefully as described in this section.

Only use the `--doformat` option to save the image that is currently in RAM into the image1 area, but be aware that this option reformats all flash partitions while saving the image.

Use the `--image[1|2]` option to save the image that is currently in RAM into a specific image area, without reformatting the partitions that contain the other image.

The following table provides more information about the `create_cf` command options, which you can view from the Linux command line by entering the name of the command.

Table A-4: Options for the create_cf command

Option	Description
none	Not recommended. Checks if a boot image is already on the device. If no image is on the device (as would be true for a newly installed removable flash on a PCMCIA card) and if no image is specified, runs --`doformat` and installs the image in image1. If multiple images are on the device, and no image is specified, presents a choice of images for the user to choose from, and then writes the image from RAM into the specified image area. In either case, restores the factory default configuration
`-d` *`device`*	Creates the image on the specified device. The default device is `/dev/hda` (the removable flash memory). Make sure the filesystem is not mounted. Use the `-d` device option if you want to create the image in another location, such as an installed compact flash PCMCIA card. (The device names for PCMCIA cards are determined by the number of the card slot where the card is installed, either `/dev/hdc` (PCMCIA slot 1) or `/dev/hde` (PCMCIA slot 2).
`--factory_default`	Creates the image with factory default configuration values. By default, if this option is not entered, the configuration from the current partition is used, if valid.
`--doformat`	Rebuilds the partitions, erasing their contents. Creates the image as image1.
`--dontformat`	Does not format the compact flash. The sizes of partitions hda1-3 and 5-8 are checked. If the partition sizes are not smaller than 2, 2, 5, 51, 51, 6, and 6 Mbytes respectively, the image is installed in the specified image area.

Table A-4: Options for the create_cf command (Continued)

Option	Description
`--image`*N*	Creates/replaces image*N*, when n=1 | 2. Use this option to replace only the specified image without erasing both images. Changes the `currentimage` environment variable to boot from the image.

Examples for create_cf Command Usage

All the examples assume you have done a network boot and you want to save the image from RAM.

Saving an Image to a Flash PCMCIA Card

After inserting a flash memory PCMCIA card into PCMCIA slot 1, you would enter the following command to save a copy of the image from RAM into the flash memory PCMCIA card in PCMCIA slot 1.

```
[root@OnSite /]# create_cf --/dev/hdc --image1
```

Saving an Image into the Image2 area and Restoring the Factory Default Configuration.

The following command saves the image from RAM into the image2 area and restores the factory default configuration.

```
[root@OnSite /]# create_cf --factory_default --image2
```

Options for the restoreconf Command

As described in other sections of this chapter, you may need to use the `restoreconf` command while troubleshooting. All the `restoreconf` subcommands are shown in the following screen example.

```
restoreconf:

Usage:

Restore from flash:           restoreconf

Restore from factory default: restoreconf factory_default

Restore from storage device:  restoreconf sd

Restore from local file:      restoreconf local <FILE>

Restore from FTP server:      restoreconf ftp <FILE>
<FTP_SERVER> <USER> <PASSWORD>

Restore from TFTP server:     restoreconf tftp <FILE>
<TFTP_SERVER>

Restore from SSH server:      restoreconf ssh <FILE>
<SSH_SERVER> <USER>
```

Glossary

1U

One rack unit (also referred to as 1RU). A standard measurement equal to 1.75” (4.45 cm) of vertical space on a rack or cabinet that is used for mounting computer equipment.

3DES

Triple Data Encryption Standard, an encrypting algorithm (cipher) that encrypts data three times, using a unique key each time, to prevent unauthorized viewers from viewing or changing the data. 3DES encryption is one of the *security features* provided by Cyclades products to enable customers to enforce their data center security policies. See also *authentication*, *authorization*, and *encryption*.

ActiveX

A set of technologies developed by Microsoft from its previous OLE (object linking and embedding) and COM (component object model) technologies. Browsers used for accessing KVM output from devices connected to Cyclades AlterPath KVM products must have ActiveX enabled.

advanced lights out manager (See *ALOM*)

AH (*authentication header)*

One of the two main protocols used by IPSec. (*ESP* is the other.) AH authenticates data flowing over the connection. AH is not compatible with *NAT*, so it must be employed only when the source and destination networks can be reached without NAT. Does not define the authentication method that must be used.

alias

An easy-to-remember, usually-short, usually-descriptive name used instead of a full name or IP address. For example, on some Cyclades products, port names contain numbers by default (as in Port_1) but the administrator can assign an alias (such as *SunBladeFremont* that describes which server is connected to the ports. Aliases make it easier for users to understand which devices are connected.

ALOM (advanced lights out manager)

A service processor on certain Sun servers that includes an independent system controller and firmware. Provides remote monitoring, logging, alerting, and basic control of the server.

application-specific integrated circuit (See *ASIC*)

ASIC (Application-Specific Integrated Circuit)

Pronounced “ay-sik”. A type of chip used for applications that provide a specific function, such as an ASIC chip that serves as a *BMC*.

authentication

The process by which a user’s identity is checked (usually by checking a user-supplied username and password) before the user is allowed to access requested resources. Authentication may be done locally (on the Cyclades device) or on a configured authentication server running one of the widely-used authentication protocols (LDAP, RADIUS, TACACS+, NIS, SMB, and Kerberos) that are supported by Cyclades products. Authentication is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. See also *authorization* and *encryption*.

authentication header (See *AH)*

authorization

Permission to access a controlled resource, which must be granted by administrative action. A user’s authorizations are checked after a user logs into a system and has been authenticated. Each user is restricted to using only the features the user is authorized to access. Checking a user’s authorizations

is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. A user who is authorized to access a device or software function is referred to as an *authorized user.* See also *authentication* and *encryption*.

authorized user

One who is given permission to access a controlled resource, which must be granted by administrative action.

backup configuration

On Cyclades products, specifies where to save compressed configuration files for possible later restoration. Some Cyclades products save configuration changes in the affected configuration files while maintaining a backed-up compressed set of configuration files in a separate directory. The backup directory's contents are available for restoration until the administrator takes a specific action to overwrite the backed-up files.

baseboard

A gender-neutral term for "motherboard."

baseboard management controller (See *BMC*)

basic input/output system (See *BIOS*)

baud rate

Pronounced "bawd rate." When configuring terminal or modem settings on serial ports and console port connections on AlterPath devices, the specified baud rate must match the baud rate of the connected devices.

Options range from 2400–921600 bps. 9600 is the most-common baud rate for devices.

BIOS (basic input/output system

Pronounced “bye-ose.” Instructions in the onboard flash memory that start up (boot) a computer without the need to access programs from a disk. Sometimes used for the name of the memory chip where the start-up instructions reside. BIOS access is available even during disk failures. Administrators often need to access the BIOS while troubleshooting, for example, to temporarily change the location from which the system boots in case of a corrupted operating system kernel. How to access the BIOS varies from one manufacturer to the other.

BMC (baseboard management controller)

An internal processor on some servers that is separate from the main system and that operates even if the main processor is not operable. Sits on the server’s baseboard (motherboard), on an internal circuit board, or on the chassis of a blade server. Monitors on-board instrumentation. Provides remote reset or power-cycle capabilities. Enables remote access to BIOS configuration or operating system console information. In some cases provides *KVM* control of the server. Includes a communication protocol that delivers the information and control to administrators.

bonding

See *Ethernet bonding*.

callback

A *security feature* used to authenticate users who are calling into a device. The software authenticates the user, hangs up, and then returns the call to the user before allowing access.

CAT5 (category 5)

A standard for twisted-pair Ethernet cables defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA).The support for CAT5 and later cabling (such as CAT5e) in many Cyclades products allows the use of existing cabling in the data center.

CDMA (code division multiple access)

A mobile data service available to users of CDMA mobile phones.

CHAP (challenge handshake authentication protocol)

An authentication protocol used for PPP authentication. See MS-CHAP.

checksum

Software posted at the Cyclades download site is accompanied by a checksum (`*.md5`) file generated using the MD5 algorithm. The checksum of a downloaded file must be the same as the checksum in the file. The checksum is compared automatically when the download is performed through the Web Manager or can be compared manually if the download is performed using `ftp` or `http`. If the checksums do not match, the software file is damaged and should not be used.

CLI (command line interface)

Allows users to use text commands to tell computers to perform actions (in contrast to using a GUI). The user types a text command at an on-screen prompt and presses the Enter or Return key. The computer processes the command, displays output when appropriate, and displays another prompt. Users can save a series of frequently-used commands in a script. Being able to create and run scripts to automate repetitive tasks is one of the reasons many administrators prefer using a CLI.

Cyclades products run the Linux operating system, and most Cyclades products allow access to the command line of the Linux shell. Command line access is achieved through several different means. For one example, a remote administrator can use Telnet or SSH to access an AlterPath OnBoard and then can enter commands on the Linux shell's command line.

Some Cyclades products offer a management utility called the CLI. Administrators type “CLI” or “cli” at the prompt in the Linux shell. Products that provide similar utilities with different names, such as the `cycli`, provide an alias for users who are familiar with the CLI name. The Cyclades CLI tool provides many commands and nested parameters in a format called the *CLI parameter tree*.

CLI parameter tree

Each version of the Cyclades *CLI* utility has a set of commands and parameters nested in the form of a tree. The CLI for the AlterPath OnBoard and other products use the Cyclades Application Configuration Protocol (CACP) daemon (cacpd). The cacpd uses the `param.conf` file, which defines a different CLI parameter tree for each product.

client-side management software—See *management software*

command line interface (See *CLI*)

community name

A string used as a type of shared password by *SNMP* v1 and v2 to authenticate messages. Hosts that share the same community name usually are physically near each other. The administrator must supply a community name when configuring SNMP on the Cyclades device, and the same community name must be also configured on the SNMP server. For security reasons, the default community name *public* should not be used.

console

A computer mode that gives access to a computer's command line (see *command line interface*). The console also displays error messages generated by the computer's operating system or *BIOS*. Console access is essential when a device (such as some special-purpose servers, routers, service processors, and other embedded devices) has no window system. Console access is also essential when the window system is not available on a device that has one, either because the system is damaged or it is offline. Access to the console allows remote administrators to control and repair damaged or otherwise-unavailable systems. See also *device console* and *service processor* console.

console servers

Appliances that give consolidated access to the console ports of connected assets, either over the network, through dial-in, or direct serial connection.

Cyclades

A corporation founded in 1989 to provide unique networking solutions. Named after the ground-breaking French packet-switching network created in 1970, which was named after the Greek province of Cyclades. Cyclades in Greece is made up of many islands that when viewed on a map resemble a diagram of nodes in a computer network.

decryption

Decoding of data that has been encrypted using an *encryption* method.

Dell Remote Assistant Cards (See *DRAC*)

Dell Remote Administrator Controller (See *DRAC*)

device console

The console on a server or another type of device that allows access to its console through an Ethernet port that is connected to one of the OnBoard's private Ethernet ports.

DHCP (dynamic host configuration protocol)

A service that can automatically assign an IP address to a device on a network, which saves administrator's time and reduces the number of IP addresses needed. Other configuration parameters may also be managed. A DHCP server assigns a dynamic address to a device based on the *MAC address* of the device's Ethernet card. Many Cyclades devices are shipped with DHCP client software, and with DHCP enabled by default.

dial-in

A method of connecting to a remote computer using communications software, such as *PPP*, along with a modem, and a telephone line, which is supported on many Cyclades products. After the administrator of the Cyclades product has connected a modem from the Cyclades product to a live telephone line and made the phone number available, a remote authorized user can use the phone number to dial into the Cyclades product and access connected devices.

DNS (domain name service or system)

A service that translates domain names (such as `cyclades.com`) to network IP addresses (192.168.00.0) and that translates host names (such as "onboard") to host IP addresses (192.168.44.11). To enable the use of this service, administrators need to configure one or more DNS servers when configuring AlterPath devices.

DRAC (Dell Remote Access Controller)

All of the following combinations are used for defining this acronym, with multiple definitions appearing even at the Dell website: Dell Remote [Access | Administrator | Administration] [Controller | Card].

Service processors on certain Dell servers may include an independent DRAC system controller. Several incompatible version types exist (DRAC II, DRAC III, DRAC III/XT, DRAC IV) along with several incompatible firmware versions. All controller types have a battery and can have an optional PCMCIA modem installed. Provide remote monitoring, logging, alerting, diagnostics, and basic control of the server. Some types have a *native web interface* and a *native application* "Dell OpenManage Server Administrator," that runs on the remote administrator's computer. Dell Open ManageIT Assistant software on the administrators computer can be used to configure and launch access.

The OnSite provides access to many but not all DRAC management functions on supported DRAC versions. To access all the management functions available through DRAC requires *native IP* access.

encapsulating security payload (See *ESP*)

encryption

Translation of data into a secret format using a series of mathematical functions so that only the recipient can decode it. Designed to protect unauthorized viewing or modification of data, even when the encrypted data is travelling over unsecure media (such as the Internet). See 3DES and SSH. As an example, a remote terminal session using secure shell SSH usually encrypts data using 3DES or better algorithms. Encryption is one of the security features provided on Cyclades products to enable customers to enforce their data center security policies. See also *authentication* and *authorization*.

ESP (encapsulating security payload)

One of the two main protocols used by IPSec (*AH* is the other). ESP encrypts and authenticates data flowing over the connection. Does not define the authentication method that must be used. DES, 3DES, AES, and Blowfish are commonly used with ESP.

Ethernet bonding

Synonymous with *Ethernet failover.* A way of configuring two Ethernet ports on a single device with the same IP address so that if the primary Ethernet port becomes unavailable, the secondary Ethernet port is used. When bonding is enabled, the active IP address is assigned to bond0 instead of eth0. When the primary Ethernet port returns to active status, the software returns it to operation.

Ethernet failover

See *Ethernet bonding*. See also *failover.*

event log

Referred to as the system event log (SEL) on most service processors, a timestamped record of events such as power on/off, device inserts/removals/ connects/disconnects, sensor threshold events and alerts.

Expect script

A script written using `expect`, a scripting language based on Tcl, the Tool Command Language. Can be written to perform automation and testing operations that are not possible with other scripting languages. Cyclades uses `expect` scripts in some of its AlterPath products, and users can customize some of the default expect scripts. For example administrators of the AlterPath OnBoard can customize the Expect scripts that handle conversations with service processors and other supported devices.

failover

A high-availability feature that relies on two redundant components in a system or a network, with the second component available to automatically take over the work of the primary components if the primary component becomes unavailable for any reason. When the primary component becomes available, it takes over the work again. Automatically and transparently redirects requests from the unavailable component to the backup component. Used to make systems more fault-tolerant. See *Ethernet bonding*.

flash memory

A chip used to store the operating system, configuration files, and applications on some Cyclades products.

GPRS (general packet radio service)

A mobile data service available to users of GSM mobile phones that adds packet data capabilities.

GSM (global system for mobile communications)

Originated by the GSM (Groupe Special Mobile) group in France in 1982. A popular standard for mobile phones.

GUI

Graphical user interface (pronounced GOO-ee). A computer interface that allows users to tell computers to perform actions by clicking on graphical elements such as icons, choosing options from menus, and typing in text fields on forms displayed on the computer screen. Many Cyclades products provide GUI access through the Cyclades Web Manager.

HTTP (hypertext transfer protocol)

Protocol defining the rules for communication between Web servers and browser across the Internet.

HTTPS (secure HTTP over SSL)

Protocol enabling the secure transmission of Web pages by encrypting data using SSL encryption. URLs that require an SSL connection start with https.

IETF (Internet Engineering Task Force)

Main standards organization for the Internet. Working groups create Internet Drafts that may become RFCs. RFCs that are approved by the Internet Engineering Steering Group (IESG) may become standards. RFCs (Requests for Comments) are the official technical specifications of the Internet protocol suite. For example, the format of SNMP MIBs was defined by the IETF, which assigns MIB numbers to organizations.

iLO (Integrated Lights Out)

Hewlett Packard's proprietary service processor (pronounced *EYE-loh*). Even though HP is a major supporter of IPMI, the company also provides iLO because it provides many more functions than IPMI. The iLO processor resides on the *baseboard*. Even if the server is off, iLO is active. When the dedicated Ethernet port is plugged into the network, iLO uses DHCP. iLO has a web interface and a Telnet interface. Advanced iLO provides remote KVM and *virtual media* access.

integrated lights out (See *ILO*)

IP address consolidation

Provides controlled access to basic management features on multiple Ethernet-based servers that have embedded service processors, using only one Internet address. When managed separately, each service processor needs its own IP address. Managing multiple servers with multiple IP addresses is both expensive and time consuming without consolidation.

IPDU (intelligent power distribution unit)

A device with multiple power inlets into which IIT assets can be plugged for remote power management. Cyclades supports a family of AlterPath PM

IPDUs that can be remotely managed when they are connected to AlterPath devices, such as the AlterPath KVM/net or AlterPath OnBoard.

IPMI (Intelligent Platform Management Interface)

An open standards vendor-independent service processor currently adopted by many major server platform vendors. Its main benefit over other service processor types is that it is installed on servers from many vendors, providing one interface and protocol for all servers. Its main disadvantage is that it does not always provide as much functionality as the proprietary service processors. For this reason, IBM's series e325 and e326 servers use IPMI to manage their BMCs but the top-of-the-line xSeries servers use *RSA II*. IPMI works by interacting with the *BMC*, and since it usually has standby power, it can function even if the operating system is unavailable or if the system is powered down. The OnSite supports IPMI version 1.5. OnSite administrators can create custom *Expect* scripts to support IPMI 2.0.

ipmitool

A command line utility that interfaces with any *BMC* that supports either IPMI 1.5 or 2.0 specifications. Reads the sensor data repository (SDR) and prints sensor values, displays the contents of the System Event Log (SEL), prints Field Replaceable Unit (FRU) inventory information, reads and sets LAN configuration parameters, and performs remote chassis power control. Described at SourceForge at: `http://ipmitool.sourceforge.net`. The command options are described on the `ipmitool`(1) man page at SourceForge: `http://ipmitool.sourceforge.net/manpage.html`. `ipmitool` commands can be added to customized scripts on the OnSite to access unsupported features on a connected service processor.

IPSec (Internet protocol security)

A suite of protocols used for establishing private, secure, connections over IP networks. Only the sending and receiving computers need to be running IPSec. Each computer handles security at its end and assumes that the intermediary nodes between the source and destination computers are not secure. Supported on many AlterPath products. In tunnel mode, IPSec is used to form a *VPN* connection, creating a secure tunnel between either an individual host or a subnet on one end and the AlterPath device on the other

end. Has two modes, *transport* and *tunnel* mode. Tunnel mode encrypts the entire packet. Transport mode encrypts application headers, TCP or UDP headers, and packet data, but not the IP header. The method that encrypts the entire packet cannot be used where NAT is required

Kerberos

Network *authentication* protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

KVM

Remote keyboard, video [monitor], and mouse access to a server through a PS/2 or USB connection on a server that is connected to a KVM switch.

KVM analog switch

A *KVM switch* that requires a local user connection before a user can gain access to any servers that are connected to the switch. Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

KVM over IP switch

A *KVM switch* that supports remote access over a LAN or WAN or telephone line to servers connected to the switch, using the TCP/IP protocols and a web browser. Enables operations over long distances. Cyclades AlterPath KVM/IP switches are one component of the *out-of-band infrastructure*.

KVM switch

Enables use of only one keyboard, video monitor, and mouse to run multiple servers from a remote location. Reduces expenses by eliminating the cost of acquiring, powering, cabling, cooling, managing, and finding data-center space for one keyboard, monitor, and mouse for every server. Servers are connected to KVM ports on Cyclades AlterPath KVM switches using AlterPath KVM terminators on the server end and up to 500 feet of *CAT5* or greater cable. AlterPath KVM switches provide *authentication* and other *security features* and allow only *authorized users* to access a restricted set of connected servers. See also *KVM analog switch* and *KVM over IP switch*. Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

LDAP (lightweight directory access protocol)

A directory service protocol used for authentication. One of many standard authentication protocols supported on Cyclades devices.

MAC address

Also called the Ethernet address. A number that uniquely identifies a computer that has an Ethernet interface. Cyclades equipment displays MAC addresses on a label on the bottom.

management console—See service processor

management network

A network separated from the *production network* that provides remote *out-of-band* access for management of IT assets, including access for returning disconnected IT assets to service without the need for a site visit.

management software

Each server company that offers a service processor produces its own client-side software to access the servers' management features through the service processor. In some cases, management software is imbedded in the service processor and is presented either as a web interface or as a command line interface accessed using SSH or Telnet, or as both a web interface and command line interface. In other cases, the management software is installed in a client workstation and accesses the management features of the service processor using an IP-based protocol, such as *IPMI*. Most of these types of software only manage one server, do not scale, and do not address the need for consolidated access-control, multi-user access, data logging, and event detection, encyrption and other needs. The OnSite addresses these needs and provides a single interface to access basic features of multiple-vendors' service processors.

MIB

Each *SNMP* device has one or more MIBs (management information bases), which describes the device's manageable objects and attributes. The MIB name tree for Cyclades starts at 1.3.6.1.4.1.4413.

MIIMON

A value set when configuring Ethernet failure to specify how often the active interface is inspected for link failures. A value of zero (0) disables MII link monitoring. A value of 100 is a good starting point, according to SourceForce bonding documentation.

MS-CHAP (Microsoft challenge handshake authentication protocol)

The Microsoft version of CHAP, which does not require the storage of a clear or reversibly-encrypted password. Can be used with or without AAA (authentication, authorization, and accounting). If AAA is enabled, PPP authentication can be done by TACACS+ and RADIUS.

NAT

Network address translation, an Internet standard that enables the use of one set of IP addresses for internal traffic and another set of IP addresses for traffic over the public network. The AlterPath OnBoard uses NAT to allow access to service processors and managed devices while not revealing their Ethernet addresses. Users can use administratively-assigned virtual IP addresses to access the service processor or device through the OnBoard.

native applications

A management option that gives the user the ability to run *service processor*-specific *native applications* and access the application's management features from the user's remote computer through the OnBoard. For example, the IBM service processor provides the IBM Director native application.

To obtain this type of access, the authenticated and authorized user selects the "Native IP" option after establishing a VPN connection between the user's computer and the OnBoard. At that point, the user can bring up the management application from where it resides on the user's computer or on the service processor and use the service processor's server management functions.

n*ative command interface* (See *NCI*)

native IP

A management option that the OnBoard administrator can enable when configuring a *service processor*. Because this option provides full access to all

features supported by the service processor, the user must be a trusted user who is specifically authorized to use the option. A *VPN* connection must be made before the user is allow to access the native IP option. When the OnSite user activates Native IP for a service processor, the OnSite routes packets between that user's IP address and the service processor through a secure tunnel. The VPN connection must remain active for the duration of the Native IP session. Authorizing a user for native IP gives the user access to a *native application* or a *native web interface* that may be provided by the service processor and that may provide additional management functions beyond those provided by the OnBoard, including *KVM over IP* access to the server.

native web interface

A service processor feature that allows browser access to the service processor's information, management, configuration, and actions, by means of a HTTP/HTTPS server running on the service processor. Access to this feature requires the user to be authorized for *native IP.*

NCI (native command interface)

A *service processor* feature that allows direct access to the *console* of the service processor. Access may be provided to features such as power control, hardware auditing, event logs, sensor readings, and service processor configuration, usually by means of a Telnet or *SSH* server running on the service processor.

NEBS (Network Equipment Building System) Certification

Means that equipment has been tested and proven to meet the NEBS requirements for central office equipment that is adhered to in common by several telecommunications carriers. The requirements are in place to ensure that telecommunications equipment poses no risk or safety hazard to people, nearby equipment, or to the physical location where the equipment operates, and that equipment is reliable and dependable during both normal and abnormal conditions. Tests address heat release, surface temperature, fire resistance, electromagnetic capability, electrical safety, and manufacturing component characteristics, among other attributes.

network time protocol (See *NTP*)

netmask

The dotted-decimal expression that determines which portion of an IP address represents the network IP address and which is used for host IP addresses, for example, 255.0.0.0.

NIS (Network Information Service)

A directory service protocol used for authentication in UNIX systems. One of many standard authentication protocols supported on Cyclades devices.

NTLM (NT LAN manager)

An authentication protocol used by Microsoft *SMB*.

NTP (network time protocol)

A protocol used to synchronize the time in a client with a high-accuracy network time protocol server.

OID

A unique indentifier for each object in an *SNMP MIB*. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the IETF, which grants authority for parts of the OID name space to individual organizations. Cyclades has the authority to assign OIDs that can be derived by branching downward from the node in the MIB name tree that starts at 1.3.6.1.4.1.4413.

SNMP programs use the OID to identify the objects on each device that can be managed by using SNMP.

onbdshell

The OnBoard shell, `/usr/bin/onbdshell`, which displays a menu of devices an authorized user can access. Accessed by authorized users through selecting the “Access Devices” option from the user shell menu, *`rmenush`*. Selecting a server name from the menu brings up the list of actions the user is authorized to perform on that server’s *service processor*. Accessed by administrators by typing`/usr/bin/onbdshell` on the OnSite’s command line; the administrators’ version of the menu lists all configured devices.

OOBI (Out-of-band Infrastructure)

An integrated systems approach to remote administration. Consists of components that provide secure, *out of band* access to connect to and manage an organization's *production network*. Components can include console servers, KVM and *KVM over IP* switches, power control appliances, centralized management devices (to control the entire out-of-band infrastructure), and service-processor managers to manage access to multiple vendor's service processors. Allows administrators to remotely connect to disconnected IT assets and to quickly return them to normal operation. Cyclades AlterPath products are designed as building blocks for an OOBI, including AlterPath ACS console servers, AlterPath KVM and KVM over P switches, AlterPath OnSite with consolidated console and KVM ports, AlterPath PM IPDUs, the AlterPath OnBoard service- processor manager, and the AlterPath Manager for centralized control of and access through multiple AlterPath devices to up to 5000 connected devices, and for access to servers that have IPMI controllers.

OTP (one-time passwords)

An authentication system that requires the user to generate and use a new password for every connection. The OTP can only be used once, which ensures that a discovered password is useless. Originally developed at Bellcore (now Telcordia), it started as a freely available program called S/Key that was trademarked. A newer freeware OTP program is OPIE (one-time passwords in everything).

out of band

Access to IT assets that is either separate from or independent of the normal *production network.* A term that originated in the telecommunications industry to refer to communications used to control a phone call that are made on a dedicated channel, which is separate from the channel over which the call is made. Allows remote monitoring and control even when a managed IT asset loses connection to the production network. Typically, out-of-band access is through a *console* or management port (typically an RS-232 or Ethernet port), an *intelligent power management device* (IPDU), a *KVM* port, or a *service processor.*

point to point protocol (See *PPP*)

point to point tunneling protocol (See *PPTP*)

PPP (point to point protocol)

A method that creates a connection between a remote computer and a Cyclades device and enables a remote user access using the Web Manager or the command line. Supports the use of the PAP, SPAP, CHAP, MS-CHAP, and EAP authentication methods.

PPTP (point to point tunneling protocol)

A *VPN* method developed by Microsoft along with other technology companies, it is the most widely supported VPN method among Windows clients and the only VPN protocol built into Windows 9x and NT operating systems. Uses the same types of authentication as PPP.

production network

The network on which the primary computing work of an organization is done. Users on a production network expect 24/7/365 availability with access to data and resources as reliable as access to telephone service. Development and testing of new applications are often performed on separate networks to avoid burdening or compromising the production network. Organizations often set up separate *management networks* to provide remote *out-of-band* access to disconnected IT assets.

RADIUS (remote authentication dial in user service)

A widely-supported authentication protocol for centralized user administration. Used by many Internet Service Providers (ISPs) and by devices such as routers and switches that do not have much storage. Combines authentication and authorization in a user profile. Relies on the UDP protocol. One of many standard authentication protocols supported on Cyclades devices.

remote supervisor adapter II (See *RSA II*)

remote system control (See *RSC*)

rmenush

The default login shell for users (`/usr/bin/rmenush`), which allows users only a limited set of menu options, including: access to management actions on devices for which they are authorized; the ability to change the user's password; and the ability to logout. The OnSite administrator may modify the menu options and commands.

RSA II (remote supervisor adapter II)

Service processor technology on certain IBM servers that includes a service processor PCI card used to manage the BMC that is located on the motherboard. Enables the remote administrator to receive notifications, alerts, to view event logs and the last screen before a failure, to use virtual media (also called "remote media"), to control power and to manage the console through a web browser using a built-in Web server. Provides more options than the IPMI service processor that is available on IBM xseries e325 and e326 servers.

RSC (remote system control)

Service processor technology on certain Sun servers that includes a *service processor* RSC card. Enables the remote administrator to run diagnostic tests, view diagnostic and error messages, reboot the server, and display environmental status information from a remote console even if the server's operating system goes offline. The RSC firmware runs independently of the host server, and uses standby power drawn from the server. The RSC card on some servers include a battery that provides approximately 30 minutes of power to RSC in case of a power failure.

secure rack management (See *SRM*)

security features

Cyclades products provide security features, including *encryption*, *authentication*, and *authorization*, to enable customers to enforce their data

center security policies while providing *out-of-band* access to managed systems.Also provided in most Cyclades products are *security profiles*.

security profiles

Most Cyclades products require the administrator to select a security profile during initial configuration, which helps enforce the security policies of the organization where the unit is being used. The security profiles are configurable and control which network services are turned on, whether a default authentication method is specified for all subsequently-configured devices, whether authorizations are checked. (Bypassing authorizations is not available in any of the default security profiles but can be selected in a custom security profile.) The security profile chosen during initial configuration can be changed later. Services can also be turned on and off independently from the security profile.

SEL (See *event log*)

serial over LAN (See SoL)

service processor (See SP)

service processor console

The console on a service processor whose dedicated Ethernet port is connected to one of the OnBoard's private Ethernet ports. Sometimes referred to as NCI (for native command interface). [OnBoard only]

service processor manager

An *OOBI* component that provides to users and groups secure, controlled access to basic features required for out-of-band management of servers that have embedded management controllers (also called *BMC*s or *service processors*). Also provides access to the console of servers and other devices without service processors but that have Ethernet ports that allow console access. Provides a single point of access through a single Ethernet address (see *IP address consolidation*) to services that are provided by service processors from several different vendors and to the console of certain servers and other devices. Its administrators are able to use a single interface to manage multiple servers without having to learn multiple management interfaces. The AlterPath OnBoard is the Cyclades service processor manager.

shell

A command interpreter on UNIX-based operating systems (like the Linux operating system that controls most Cyclades products). A shell typically is accessed in a terminal window where the shell presents a prompt. For example: `[admin@OnSite admin]#` is the prompt that appears when a user logs into an OnSite as admin and is in the `/home/admin` directory. Users tell the operating system to perform actions by typing commands in the shell, which interprets the commands and performs the specified actions. See also *command line interface*. The AlterPath OnSite has two user shells: *`onbdshell`* and *`rmenush`*.

simple mail transfer protocol (See *SMTP*)

SMB (server message block)

A protocol used for file sharing and other communications between Windows computers. Microsoft uses this protocol along with NTML authentication protocol used to authenticate a client on a server.

SMTP (simple mail transfer protocol)

The most-commonly-used protocol used to send email.

SNMP (simple network management protocol)

A set of network management protocols for TCP/IP and IPX (Internet Packet Exchange) networks, which are part of the TCP/IP protocol suite. Supports management of devices running SNMP agent software by remote administrators using *SNMP manager software*, such as HP OpenView, Novell NMS, IBM NetView, or Sun Net Manager, on remote computers. Devices running SNMP agent software send data from management information bases (*MIBs*) to the SNMP manager software.

On certain Cyclades devices, administrators can enable SNMP to allow a remote administrator to manage the device and can configure the device to send alerts about events of interest. Before enabling SNMP, the administrator needs the following information: The contact person (administrator) of the AlterPath device; the physical location, the *community name* (for SNMP v1, v2c only), IP address or DNS hostname of the *SNMP manager*. The OnBoard supports SNMP v1, v2c, and v3. The SNMP configuration file is located at `/etc/snmp/snmpd.conf`. See also *OID* and *traps*.

SNMP manager

Any computer running SNMP manager software. Also called a network management station or SNMP server.

SNMP manager software

Displays data about managed devices on the console or saves the data in a specified file or database. Some network management programs such as HP OpenView graphically show information about managed devices.

SNMP server (See SNMP manager)

SoL *(*serial over LAN)

Access to the console of a server or other device that supports redirection of serial server data to a dedicated Ethernet port. Permits access to and control of the BIOS and operating system console over the LAN or Internet. Eliminates the need for the device to have a serial port and the need for serial cabling to enable console access. On the OnSite, once a device's SoL Ethernet port is connected to one of the OnSite's private Ethernet ports, an authorized user can access the server or a device's console either through the "Device console" or "devconsole" option (available on the *Web Manager*, *`rmenush`*, or *`onbdshell`*`)` or through entering the `devconsole` command with `ssh` on the command line).

SP (service processor)

Ethernet-based management controller on a server, which provides out-of-band management through an interface between the server's administrator and an internal baseboard management controller (BMC) that enables the management features. Management features can include serial console emulation (using Telnet or IPMI), *KVM over IP,* power control, sensor and log information from the server hardware, and virtual media.

SRM (secure rack management)

An out-of-band infrastructure (OOBI) capability delivered by the AlterPath OnSite that isolates the management ports (emergency service ports) of servers that have *service processors* from the *production network*. Physically consolidates and logically secures the Ethernet connections between the AlterPath OnSite and the connected service processors. By providing *IP*

consolidation, SRM substantially lowers the cost and complexity of deploying service processors. SRM also lowers the security risks of using service processors by providing centralized authentication and user access control, isolating vulnerable service processor protocols from the production network and communicating with authenticated and *authorized users* over the public network using higher-end secure protocols (such as *SSH*, *SSL*, and *HTTPS*).

SSH

Secure shell, developed by SSH Communications Security, Ltd., is a UNIX-based *shell* and protocol that provides strong authentication and secure communications over unsecured channels. Unlike `telnet`, `ftp`, and the `rcp`/`rsh`/`remsh` programs, SSH encrypts everything it sends over the network. Many Cyclades products support SSH version 1 and SSH version 2. Since SSH1 and SSH2 are entirely different, incompatible protocols, it is important when given a choice between enabling one or the other of the two SSH versions to enable the version that is available on the computer being used to access the Cyclades equipment. The OpenSSH (`www.openssh.org`) package is used on the AlterPath OnSite. THe OnSite uses the Open SSH version that is certified by the Cryptographic Module Validation (CMV) program run by the U.S. National Institute of Standards (NIST) and the Canadian government's Communications Security Establishment (CSE). Authorized users on the AlterPath OnSite can enter an OnSite-specific set of commands such as poweron, poweroff, powercycle when using `ssh` on the command line to perform *service processor* management actions.

SSL (secure sockets layer)

A protocol for transmitting private documents via the Internet. Also used for the type of connection used for transmitting the information. Uses two keys to encrypt data being transferred: a public key and a private or secret key known only to the message receiver. See also *HTTP/HTTPS*.

system event log (See *event log*)

TACACS+ (Terminal Access Controller Access Control System)

An authentication protocol (pronounced *tak-ak_plus*) that provides separate authentication, authorization, and accounting services. Based on TACACS, but completely incompatible with it. Uses the TCP protocol, which is seen by

some administrators as a more-reliable protocol than the UDP protocol used by RADIUS. One of many standard authentication protocols supported on Cyclades devices.

trap

An operation started by an SNMP agent in response to an event of interest on a managed-object in a device, which sends an alert to the *SNMP manager*. The administrator of certain Cyclades device can configure which types of events generate trap messages and trap destinations. Also known as SNMP messages or as “PDUs”—protocol data units.

virtual media

Emulates the use of a floppy or CD drive that is physically connected to the remote administrator’s computer to

VPN (virtual private network)

A mechanism enabling two computers to securely transfer information over an otherwise untrusted network through a secure tunnel. Two common options used for VPN are *IPSec* and *PPTP*.

Web Manager

Cyclades' web management interface. The Web Manager runs in supported browsers and allows remote administrators to configure Cyclades products and to enable remote users to access servers and other devices that are connected to Cyclades products. Authorized users can use the Web Manager to access connected devices.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y